Configuring DLSw Services

Router Software Version 10.0
Site Manager Software Version 4.0

Part No. 112914 Rev. A
January 1996

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1996 Bay Networks, Inc.

All rights reserved. Printed in the USA. January 1996.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, BCN, BLN, BN, CN, FRE, LN, Optivity, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and AN, ANH, ASN, BaySIS, BayStack, BCNX, BLNX, BNX, EZ Internetwork, EZ LAN, FN, PathMan, PhonePlus, PPX, Quick2Config, RouterMan, SPEX, Bay Networks, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks Software License

Note: *This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license — or the license included with the particular product — shall govern licensee's use of Bay Networks software.*

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

About This Guide

Audience xvii
Before You Begin xviii
Bay Networks Customer Support xviii
CompuServe xviii
InfoFACTS xix
World Wide Web xix
How to Get Help xx
Conventions xx
Ordering Bay Networks Publications xxi
Acronyms xxi

Chapter 1
Data Link Switching Overview

DLSw Networking Overview 1-2
DLSw Single and Dual Switch-to-Switch Services 1-3
DLSw Single-Switch Services 1-5
DLSw Dual Switch Services 1-6
SDLC Support 1-8
Integrated SDLC Conversion 1-9
Frame Relay Support 1-11
DLSw Filtering 1-13
Inbound Traffic Filters 1-13
DLSw Prioritization 1-13
Protocol Prioritization 1-14
DLSw and Related Protocols 1-14
For More Information about DLSw 1-15

Chapter 2
DLSw Implementation Notes

Source Route Bridge Topologies 2-1
Counting SRB LANs and Bridges 2-2
Counting the IP Virtual Ring 2-3
Counting the Internal LAN 2-6
Counting the DLSw Bridge 2-7
Computing a DLSw Connection Path 2-8
Parallel Data Paths 2-9
Multiple DLSw Peers on a LAN 2-11
DLSw and Bridging Services 2-11
DLSw on an SRB Circuit 2-11
DLSw on an Ethernet/802.3 Circuit 2-12
DLSw with Translation Bridge 2-13
Memory Requirements 2-14
TCP Considerations 2-15
DLSw Keepalive Time 2-15
TCP Max Retransmission Timeout 2-16
Flow Control 2-16
LLC2 Flow Control 2-17
TCP Flow Control 2-17
Performance 2-18
DLSw Packaging 2-18

Chapter 3
DLSw Configuration Overview

DLSw Session Setup Overview 3-1
Site Manager Roadmaps to Configuring DLSw 3-2
Configuration Objects for Single Switch DLSw 3-5
DLSw SAP Table 3-5
DLSw Slot Table 3-6
Configuration Objects for Dual Switch DLSw 3-8
DLSw Peer IP Table 3-9
Configured Peers 3-9
Simplifying the Peer IP Table 3-10
Broadcast Peers 3-10

Unconfigured Peers 3-10
Configuration Objects for SDLC 3-12
SDLC Line Parameters 3-12
Local Devices 3-14
Optional Configuration Objects 3-15
Dynamically Learned Remote Systems 3-15
Statically Defined Remote Systems 3-16

Chapter 4
Enabling DLSw Services

Enabling DLSw on an Interface 4-1
Configuring DLSw the First Time 4-2
Setting the DLSw Global Parameters 4-2
Specifying Source Routing Bridge Encapsulation 4-4
Adding Source Routing Parameters 4-4
Mapping Frame Relay Addresses 4-5
Adding Slot IP Addresses 4-7
Adding DLSw Peer IP Addresses 4-9
Adding a Service Access Point (SAP) 4-11
Editing SDLC Line Parameters and SDLC Local Devices 4-13
Subsequent DLSw Configuration 4-25

Chapter 5
Editing DLSw Parameters

Using the Parameter Descriptions 5-1
Accessing DLSw Parameters 5-2
Editing DLSw Global Parameters 5-3
DLSw Global Parameter Descriptions 5-4
Enabling a DLSw Interface 5-13
Enabling a DLSw Interface Using the Edit Circuits Function 5-14
Editing DLSw Peer IP Table Parameters 5-17
Adding a DLSw Peer IP Table Entry 5-18
Editing a DLSw Peer IP Table Entry 5-20
Deleting a DLSw Peer IP Table Entry 5-20
Editing the DLSw Slot IP Table 5-21
Adding a DLSw Slot IP Table Entry 5-22

Editing a DLSw Slot IP Table Entry 5-24
Deleting a DLSw Slot IP Table Entry 5-25
Editing DLSw SAP Table Parameters 5-26
Adding a DLSw SAP Table Entry 5-27
Editing a DLSw SAP Table Entry 5-29
Deleting a DLSw SAP Table Entry 5-31
Editing DLSw Default NetBIOS Peer IP Table Parameters 5-32
Adding a DLSw Default NetBIOS Peer IP Table Entry 5-33
Editing a DLSw Default NetBIOS Peer IP Table Entry 5-36
Deleting a DLSw Default NetBIOS Peer IP Table Entry 5-37
Editing DLSw Default MAC Peer IP Table Parameters 5-38
Adding a DLSw Default MAC Peer IP Table Entry 5-39
Editing a DLSw Default MAC Peer IP Table Entry 5-41
Deleting a DLSw Default MAC Peer IP Table Entry 5-43
Editing DLSw Local Devices Parameters 5-44
DLSw Local Devices Parameter Descriptions 5-46
Deleting a DLSw Local Device Entry 5-54
Editing DLSw Traffic Filters and Protocol Prioritization 5-54
Deleting DLSw from the Node 5-54

Chapter 6
Using DLSw Prioritization

Protocol Prioritization Overview 6-1
Two Types of Protocol Prioritization 6-2
DLSw Priority Queues 6-3
Default and Peer-Specific DLSw Queues 6-3
The Enqueuing Process 6-3
Nonordered Queues 6-4
The Dequeuing Process 6-4
The Dequeue List 6-5
Weighted Dequeuing Algorithm 6-5
Tuning DLSw Protocol Prioritization 6-7
DLSw Priority Queues and Congestion Control 6-7
Queue Depth 6-7
Configuring Default Priority Queues 6-8
Enabling the Default Queues for Configured and Unconfigured Peers 6-9

Customizing the Default Queue Configuration 6-12
DLSw Protocol Prioritization Parameter Descriptions 6-13
Configuring Peer-Specific Priority Queues 6-15
Priority Queues for a Specific DLSw Peer 6-15
Enabling or Disabling a Single Peer's Priority Queues 6-19
Customizing Specific DLSw Peer Queues 6-20
Peer Queue Configuration Parameter Descriptions 6-21
Creating DLSw Priority Filters 6-22
Using the DLSw Peer Configuration Window 6-30
Sample Templates for DLSw Protocol Prioritization 6-31

Appendix A
DLSw Default Settings

Appendix B
Criteria for DLSw Prioritization

Predefined DLSw Criteria B-2
DLSw Reference Points B-2
Specifying MAC Address Ranges B-4
Source Routing Bridge Source MAC Addresses B-4
Source Routing Bridge Functional MAC Addresses B-5
Specifying Source and Destination SAP Code Ranges B-5

Index

Figures

Figure 1-1. DLSw Single-Switch and Dual Switch-to-Switch Networks 1-4
Figure 1-2. Bay Networks Single-Switch Router 1-5
Figure 1-3. Bay Networks Adjacent Single Switch Routers 1-6
Figure 1-4. DLSw Dual Switch Services for SNA Devices on LANs 1-7
Figure 1-5. SDLC Conversion in a Single-Switch Configuration 1-9
Figure 1-6. SDLC Conversion in a Dual Switch-to-Switch Configuration 1-10
Figure 1-7. Sample Frame Relay Network 1-12
Figure 2-1. Maximum Ring and Bridge Hop Counts in a Source Routing Network 2-2
Figure 2-2. DLSw-Capable Routers on an IP Backbone 2-3
Figure 2-3. DLSw Peers Using an IP Virtual Ring 2-4
Figure 2-4. Counting the IP Virtual Ring 2-6
Figure 2-5. Router Logical Considerations for DLSw Support 2-7
Figure 2-6. End-to-End Path in a DLSw-capable Token Ring/802.5 Network 2-9
Figure 2-7. DLSw Services in Parallel with a Transparent Bridge 2-10
Figure 2-8. DLSw Services in Parallel with a Source Routing Bridge 2-10
Figure 2-9. DLSw and Source Route Bridging on SRB Circuits 2-12
Figure 2-10. DLSw and Transparent Bridging on Ethernet/802.3 Circuits 2-13
Figure 2-11. Translation Bridge Services 2-14
Figure 3-1. DLSw Configuration Sequence for Token Ring/802.5 or Other Source Route Bridge Networks 3-3
Figure 3-2. DLSw Configuration Sequence for Ethernet/802.3 or Frame Relay Network 3-4
Figure 3-3. Sample Network with SAP Table Definitions 3-6
Figure 3-4. Sample Network with Slot Table Definitions 3-8
Figure 3-5. Sample Network with Peer IP Table Definitions 3-12
Figure 4-1. DLSw Global Parameters Window 4-3
Figure 4-2. Source Route Encapsulation Dialogue Box 4-4
Figure 4-3. LLC2 Frame Relay Mappings Window 4-5

Figure 4-4. LLC2 Frame Relay Mapping Add Window 4-6
Figure 4-5. DLSw Slot Configuration Window 4-8
Figure 4-6. Add DLSw Slot Configuration Window 4-8
Figure 4-7. DLSw Peer Configuration Window 4-10
Figure 4-8. Add DLSw Peer Configuration Window 4-10
Figure 4-9. DLSw SAP Configuration Window 4-12
Figure 4-10. Add DLSw SAP Configuration Window 4-12
Figure 4-11. SDLC Line Parameters Window 4-14
Figure 4-12. Select Protocols Window 4-16
Figure 4-13. DLS Local Device Configuration Window 4-17
Figure 4-14. Local Device Configuration Window 4-18
Figure 5-1. Configuration Manager Window 5-3
Figure 5-2. Edit DLSw Global Parameters Window 5-4
Figure 5-3. DLSw Interface Configuration Window 5-13
Figure 5-4. Circuit List Window 5-15
Figure 5-5. Edit Connector Window 5-15
Figure 5-6. Circuit Definition Window 5-16
Figure 5-7. Edit DLSw Interface Window 5-16
Figure 5-8. Configured Peer in DLSw Peer Configuration Window 5-18
Figure 5-9. IP Address in DLSw Peer Configuration Window 5-19
Figure 5-10. Deleting a DLSw Peer IP Table Entry 5-20
Figure 5-11. DLSw Slot Configuration Window 5-22
Figure 5-12. IP Address in DLSw Slot Configuration Window 5-22
Figure 5-13. Saving an Edited DLSw Slot IP Address 5-24
Figure 5-14. Deleting a DLSw Slot Table Entry 5-25
Figure 5-15. SAP Addresses in DLSw SAP Configuration Window 5-27
Figure 5-16. SAP Parameter in DLSw SAP Configuration Window 5-27
Figure 5-17. Saving the Edited SAP Window Setting 5-30
Figure 5-18. Deleting a SAP Table Entry 5-32
Figure 5-19. DLSw NetBIOS Peer Configuration Window 5-33
Figure 5-20. DLSw NetBIOS Configuration Window 5-34
Figure 5-21. Saving a DLSw Default NetBIOS Peer IP Table Entry 5-36
Figure 5-22. Deleting a DLSw Default NetBIOS Peer IP Table Entry 5-38
Figure 5-23. DLSw MAC Peer Configuration Window 5-39
Figure 5-24. MAC Addresses in the DLSw MAC Configuration Window 5-40

Figure 5-25. Saving a DLSw Default MAC Peer IP Table Entry 5-42
Figure 5-26. Deleting a DLSw Default MAC Peer IP Table Entry 5-43
Figure 5-27. DLS Local Device Configuration Window 5-45
Figure 5-28. DLS Local Device Configuration Add Window 5-46
Figure 6-1. Weighted Bandwidth Allocation 6-6
Figure 6-2. Selecting DLSw Protocol Prioritization 6-9
Figure 6-3. Global DLSw PP Parameters/Defaults Window 6-10
Figure 6-4. Enabling Protocol Prioritization on DLSw Peers 6-10
Figure 6-5. Enabling PP for Unconfigured Peers 6-11
Figure 6-6. Enabling Protocol Prioritization for All DLSw Peers 6-11
Figure 6-7. Global DLSw PP Parameters/Defaults Window 6-12
Figure 6-8. Selecting the Peer Queue Entries Window 6-15
Figure 6-9. Peer Queue Configuration Window 6-16
Figure 6-10. Add/Edit/Delete Queues Window 6-17
Figure 6-11. Add Queue Window 6-17
Figure 6-12. Configured Queues 6-18
Figure 6-13. Peer Queue Configuration Window with Both Default and Peer-Specific Configurations 6-19
Figure 6-14. Peer Queue Configuration Window 6-20
Figure 6-15. Selecting the DLS Priority/Outbound Filters Window 6-22
Figure 6-16. DLS Priority/Outbound Filters Window 6-23
Figure 6-17. Filter Template Management Window 6-24
Figure 6-18. Selecting a Predefined DLSw Outbound Filter Criterion 6-25
Figure 6-19. Selecting the DLSw Queue Action 6-26
Figure 6-20. Queue Number Window 6-27
Figure 6-21. Create Filter Window 6-28
Figure 6-22. DLS Priority/Outbound Filters Window with Configured FIlters 6-29
Figure 6-23. DLSw Peer Configuration Window 6-30

Tables

Table 5-1. Customizing the DLSw Support Protocols 5-2
Table A-1. DLSw Global Parameters A-1
Table A-2. DLSw Interface Parameters A-2
Table A-3. DLSw Peer IP Table Parameters A-2
Table A-4. DLSw Protocol Prioritization Parameters A-2
Table A-5. DLSw Slot IP Table Parameters A-3
Table A-6. DLSw SAP Parameters A-3
Table A-7. DLSw Default NetBIOS Peer IP Table Parameters A-3
Table A-8. DLSw Default MAC Peer IP Table Parameters A-3
Table A-9. DLSw Local Devices Parameters A-4
Table B-1. Predefined Outbound Filter Criteria Based on DLSw Header B-2
Table B-2. DLSw Reference Points for FID2 Frames B-3
Table B-3. DLSw Reference Points for FID4 Frames B-3
Table B-4. Format for Specifying Source-Routing MAC Addresses B-4
Table B-5. Functional MAC Addresses B-5
Table B-6. SAP Codes B-6

About This Guide

This guide describes how to customize Bay Networks™ router software for Data Link Switching (DLSw) services.

The guide provides

- An overview of DLSw services on the router (Chapter 1)
- Implementation notes that may affect how you configure DLSw services on the network (Chapter 2)
- An overview of the configuration process for DLSw using the Configuration Manager software (Chapter 3)
- Instructions for enabling DLSw on Bay Networks routers (Chapter 4)
- Instructions for editing DLSw global and interface parameters, and for configuring DLSw Local Devices, Peer, Slot, and SAP tables (Chapter 5)
- Information on prioritizing DLSw traffic, configuring priority queues for DLSw peers, and applying DLSw prioritization using outbound filters (Chapter 6)
- A list of DLSw parameters and their default settings in the Configuration Manager (Appendix A)
- A list of predefined criteria and reference points for user-defined criteria for DLSw prioritization (Appendix B)

Audience

Written for system and network managers, this guide describes how to configure the Bay Networks implementation of DLSw to suit your environment.

Before You Begin

Before using this guide, you must complete the following procedures:

- Open a configuration file
- Specify the router hardware, if this is a local-mode configuration file
- Select the link- or net-module connector on which you are enabling DLSw

See *Configuring Routers* for instructions.

Bay Networks Customer Support

Bay Networks provides live telephone technical support to our distributors, resellers, and service-contracted customers from two U.S. and three international support centers. If you have purchased your Bay Networks product from a distributor or authorized reseller, contact the technical support staff of that distributor or reseller for assistance with installation, configuration, troubleshooting, or integration issues.

Customers also have the option of purchasing direct support from Bay Networks through a variety of service programs. The programs include priority access telephone support, on-site engineering assistance, software subscription, hardware replacement, and other programs designed to protect your investment.

To purchase any of these support programs, including PhonePlus™ for 24-hour telephone technical support, call 1-800-2LANWAN. Outside the U.S. and Canada, call (408) 764-1000. You can also receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your reseller. Bay Networks provides several methods of receiving support and information on a nonpriority basis through the following automated systems.

CompuServe

Bay Networks maintains an active forum on CompuServe. All you need to join us online is a computer, a modem, and a CompuServe account. We also recommend using the CompuServe Information Manager software, available from CompuServe.

The Bay Networks forum contains libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. Software agents and patches are available, and the message boards are monitored by technical staff and can be a source for problem solving and shared experiences.

Customers and resellers holding Bay Networks service contracts can visit the special libraries to acquire advanced levels of support documentation and software.

To open an account and receive a local dial-up number, call CompuServe at 1-800-524-3388 and ask for Representative No. 591.

- In the United Kingdom, call Freephone 0800-289378.
- In Germany, call 0130-37-32.
- In Europe (except for the United Kingdom and Germany), call (44) 272-760681.
- Outside the U.S., Canada, and Europe, call (614) 529-1349 and ask for Representative No. 591, or consult your listings for an office near you.

Once you are online, you can reach our forum by typing the command GO BAYNETWORKS at any ! prompt.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand service. This automated system contains libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system can return a fax copy to the caller or to a third party within minutes of being accessed.

World Wide Web

The World Wide Web (WWW) is a global information system for file distribution and online document viewing via the Internet. You need a direct connection to the Internet and a Web Browser (such as Mosaic or Netscape).

Bay Networks maintains a WWW Home Page that you can access at http://www.baynetworks.com. One of the menu items on the Home Page is the Customer Support Web Server, which offers technical documents, software agents, and an E-mail capability for communicating with our technical support engineers.

How to Get Help

For additional information or advice, contact the Bay Networks Technical Response Center in your area:

United States	1-800-2LAN-WAN
Valbonne, France	(33) 92-966-968
Sydney, Australia	(61) 2-903-5800
Tokyo, Japan	(81) 3-328-005

Conventions

This section describes the conventions used in this guide.

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
arrow character (➔)	Separates menu and option names in instructions. Example: Protocols➔AppleTalk identifies the AppleTalk option in the Protocols menu.
bold text	Indicates text that you need to enter and command names in text. Example: Use the **dinfo** command.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`

vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show at routes** | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers. You may also request a free catalog of Bay Networks Press product publications.

Phone:	1-800-845-9523
FAX - U.S./Canada:	1-800-582-8000
FAX - International:	1-916-939-1010

Acronyms

APPN	Advanced Peer-to-Peer Networking
DLSw	Data Link Switching
FDDI	Fiber Distributed Data Interface
FEP	front-end processor
FRAD	Frame Relay Access Device
FIFO	first-in/first-out
IP	Internet Protocol
LLC	logical link control
MAC	media access control
MTU	Maximum Transmission Unit
SAP	service access point
SDLC	Synchronous Data Link Control
SNA	Systems Network Architecture
SRB	source routing bridge
SSP	Switch-to-Switch Protocol

TCP/IP	Transmission Control Protocol/Internet Protocol
VTAM	Virtual Telecommunications Access Method
XID	exchange identification

Chapter 1
Data Link Switching Overview

This chapter presents information about Data Link Switching (DLSw), as follows:

- DLSw networking overview
- DLSw single and dual switch services
- SDLC support
- Frame Relay support
- DLSw filtering

You should review this chapter if you are responsible for configuring DLSw on one or more Bay Networks routers. If you are already familiar with DLSw concepts, you can go directly to Chapter 2, “DLSw Implementation Notes,” for more detailed information about DLSw on Bay Networks routers.

DLSw Networking Overview

Data Link Switching (DLSw) provides a standards-based mechanism for reliably transporting connection-oriented SNA and NetBIOS data across a network. Originally defined in RFC 1434, DLSw resolves the issues associated with transporting SNA and NetBIOS information across a multiprotocol backbone.

Specifically, DLSw:

- Prevents sessions from timing out due to slow network response time
- Automatically reroutes traffic around failed links
- Improves response time by reducing network overhead
- Enables multiple locations to interconnect without reconfiguring existing bridges

Additionally, Bay Networks DLSw implementation provides several benefits while retaining interoperability with other implementations of Data Link Switching. These benefits include

- Bay Networks symmetric multiprocessor architecture, providing a highly scalable and reliable implementation.
- Advanced flow control, ensuring that the router-based network delivers information as reliably as existing SNA networks.
- Integrated SDLC-to-LLC2 conversion, enabling the customer to reduce the cost of Front-End Processor (for example, 3745) ports, maintenance and software.
- RFC 1490 (LLC2 over Frame Relay) support, enabling a Bay Networks router to communicate across a Frame Relay network directly to a Front End Processor or other device that supports this protocol.
- DLSw Prioritization, allowing preferred traffic to receive higher priority. Up to ten priority levels can be defined, with weights assigned to each priority queue. Prioritization uses standard DLSw TCP ports without affecting multivendor interoperability.

The Bay Networks DLSw implementation is fully interoperable with the IBM 6611 Network Processor and other RFC 1434 DLSw implementations.

DLSw runs on all Bay Networks router platforms using local and wide area network facilities, including

- LAN media, including Ethernet, Token Ring, and Frame Relay
- Other LAN media using SRB formats over Ethernet, FDDI, SMDS, Frame Relay, and Point-to-Point (PPP) protocols
- SDLC links in point-to-point and multipoint configurations

You can use DLSw services to support connections between SNA and NetBIOS systems on one type of network (such as Token Ring/802.5) and systems on different types of networks (such as Frame Relay).

Note: *In this manual, the term LAN refers to all source-route-bridge types of LANs and transparent-bridge Ethernet/802.3 LANs. Source-route-bridge LANs include, but are not limited to, Token Ring/802.5, FDDI, Ethernet/802.3, SMDS, Frame Relay, and other synchronous media protocols. See* Configuring Bridging Services *for more information on the media that source route bridging supports.*

DLSw Single and Dual Switch-to-Switch Services

Bay Networks routers that you configure to support DLSw services can operate in two modes:

- A DLSw single-switch configuration involving a single local router with two (or more) interfaces configured for DLSw.
- A DLSw dual switch-to-switch configuration involving paired routers each connected to an intervening TCP/IP network.

A Bay Networks router simultaneously supports both single- and dual-switch operation. Figure 1-1 illustrates DLSw single-switch and dual switch-to-switch networks.

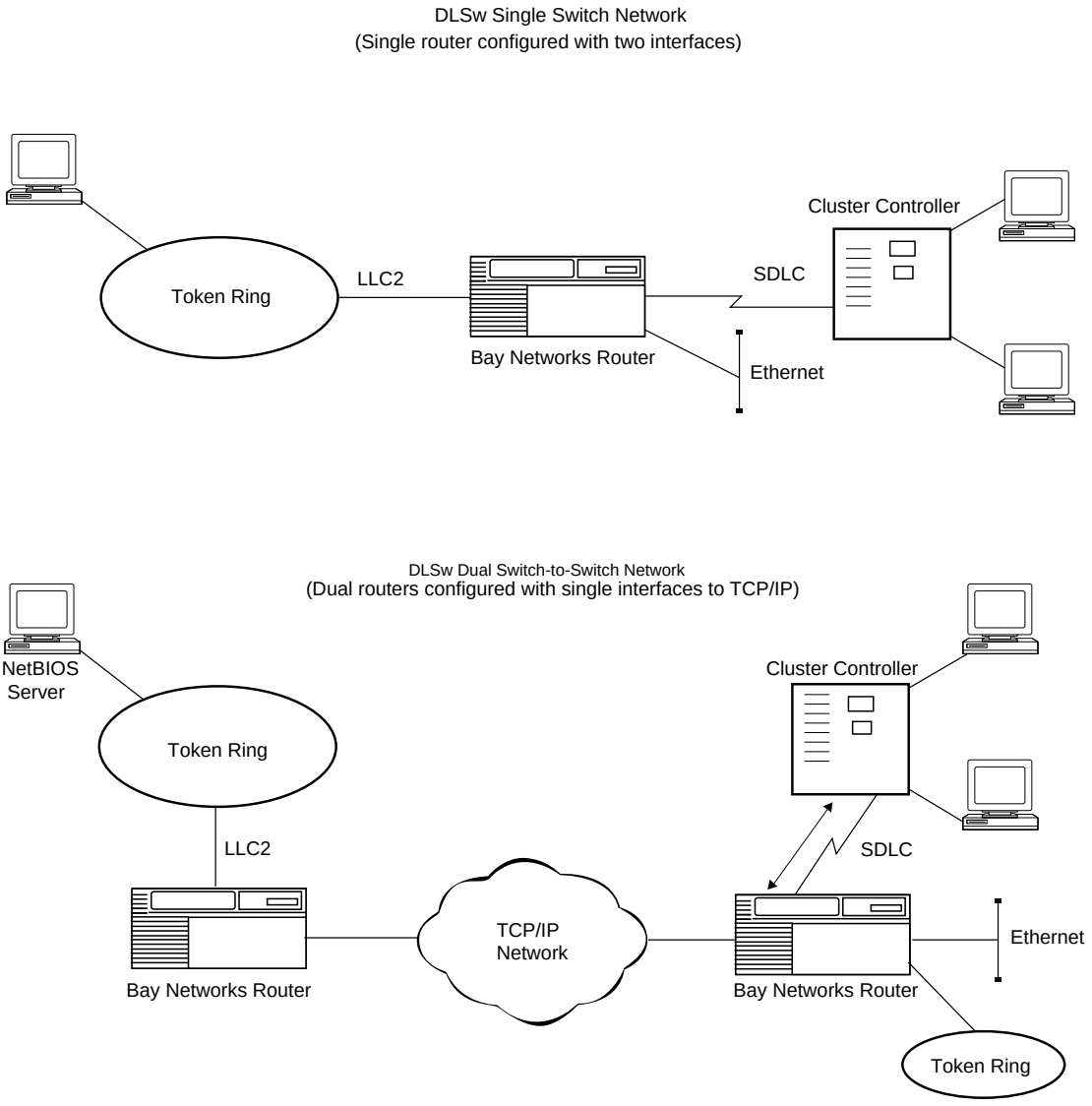


Figure 1-1. DLSw Single-Switch and Dual Switch-to-Switch Networks

DLSw Single-Switch Services

DLSw single-switch services enable the router to perform link level conversion, while providing services to ensure session integrity. Examples of single-switch conversions include

- SDLC to Token Ring
- SDLC to Frame Relay (RFC 1490)
- Token Ring to Ethernet
- Ethernet to bridged SNA over Frame Relay

Single switch configurations provide services to attached devices and networks to ensure session availability, including

- Local acknowledgment and termination of the LLC2 or SDLC session
- 802.5 routing information field (RIF) caching (allowing more than eight source-route-bridged rings between a local and remote system)
- MAC address and NetBIOS name caching

Figure 1-2 illustrates a sample network using a single Bay Networks router. The router can communicate with an IBM front end processor (FEP) or other LAN gateway.

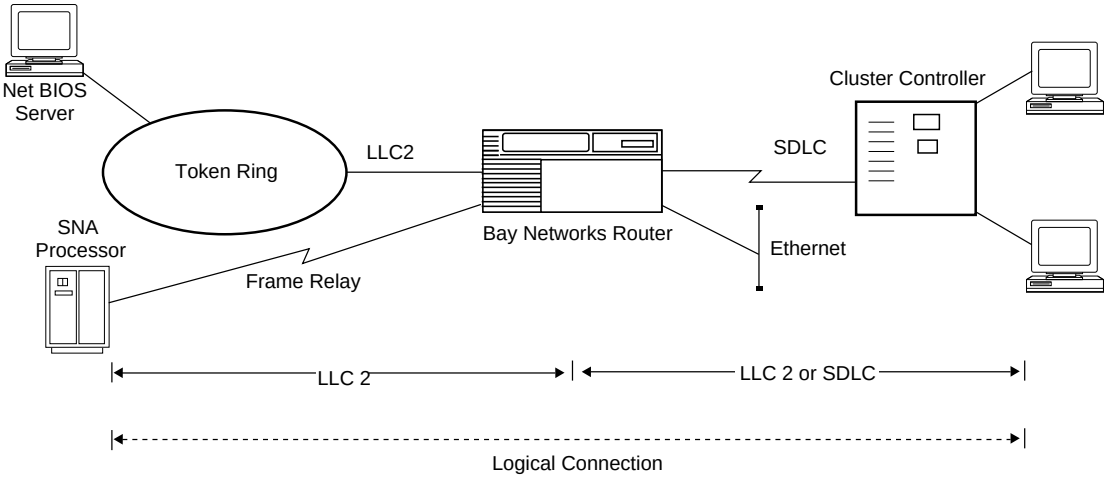


Figure 1-2. Bay Networks Single-Switch Router

Figure 1-3 illustrates a network using adjacent routers, each performing single-switch conversion. Between single switch routers, the LLC2 protocol is used.

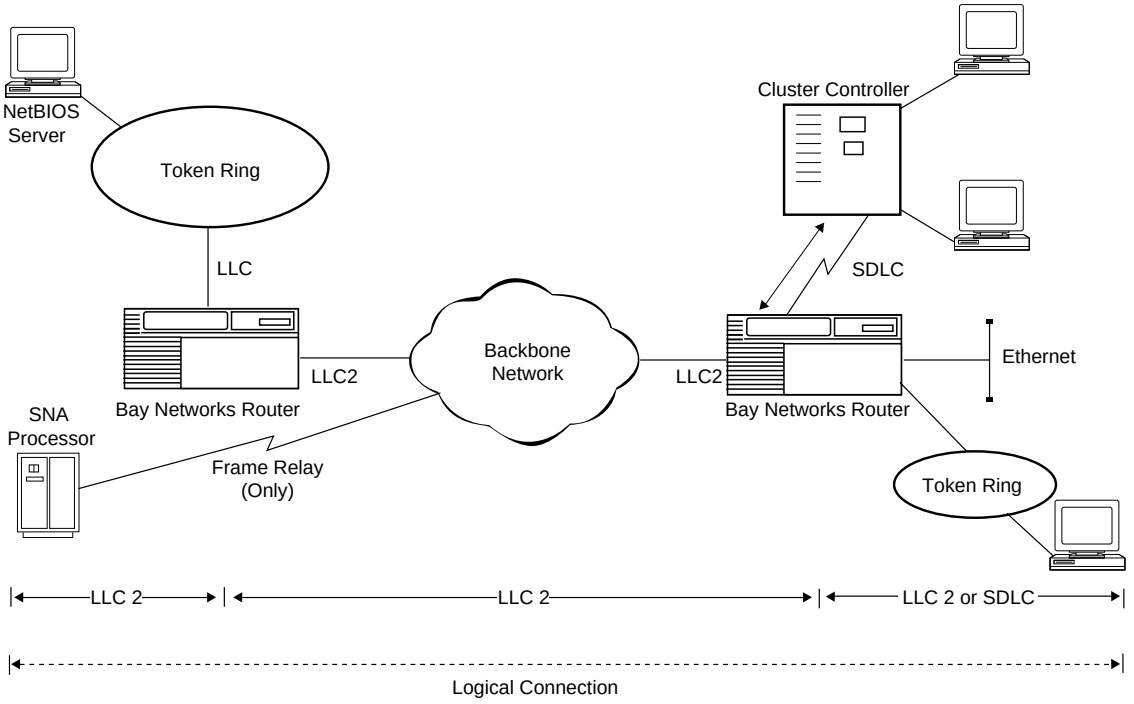


Figure 1-3. Bay Networks Adjacent Single Switch Routers

DLSw Dual Switch Services

DLSw dual switch services allows SNA and NetBIOS traffic to share a multiprotocol backbone. The DLSw standard specifies TCP/IP as the standard transport mechanism for SNA and NetBIOS across an internetwork.

DLSw dual switch services uses TCP/IP between routers, unlike adjacent single switch routers using LLC2. DLSw dual switch services provides

- IP routing, permitting delivery over any available path
- TCP services, providing reliable data delivery, reduced network overhead, and flow control mechanisms to manage traffic

DLSw dual switch services is based on RFC 1434. This RFC defines the TCP/IP control protocol, Switch-to-Switch Protocol (SSP) used between DLSw devices.

Packets from a Token Ring, Ethernet, Frame Relay, or SDLC network are carried to an attached Bay Networks DLSw node where the data is translated into SSP datagrams. The data is then routed over the multiprotocol backbone to a remote Bay Networks DLSw node using an IP routing protocol. When the SSP datagram reaches the remote Bay Networks DLSw node, it is translated into the appropriate frame and carried to its destination.

Figure 1-4 shows how SNA devices use DLSw dual switch services to communicate over TCP/IP. This differs from adjacent single switch operation, which uses LLC2 on the backbone.

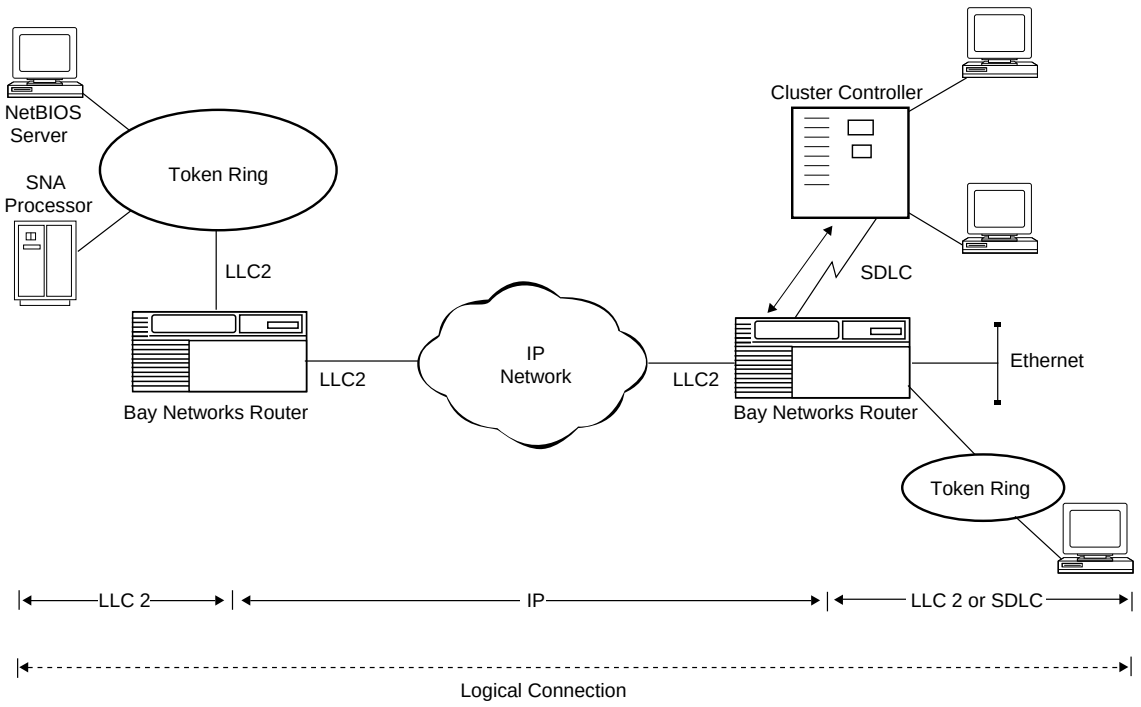


Figure 1-4. DLSw Dual Switch Services for SNA Devices on LANs

SDLC Support

The Bay Networks integrated SDLC support merges the low-speed SDLC traffic of an SNA network with the high-speed, multiprotocol traffic of LANs into a single network backbone. SDLC operates in DLSw single switch routers, or in dual switch-to-switch networks, as illustrated in Figure 1-1.

DLSw integrated SDLC supports devices configured as primary or secondary link stations to the router. Only one link station on an SDLC line can be the primary station; all other stations on the line must be secondary.

A link station is a logical connection between adjacent nodes, where one node is a primary link station and the other node is a secondary link station. SDLC supports primary and secondary link stations. A primary link station does the following:

- Controls a data link
- Issues commands
- Initiates error-recovery procedures

A secondary link station receives commands and responds to polls initiated by the primary SDLC link station.

The synchronous line speed (between the SDLC device and the Bay Networks router) can be up to 64 Kb/s.

You can use integrated SDLC in a point-to-point or multipoint topology. Point-to-point connects one SDLC device to the SDLC port. Multipoint connects several SDLC devices to the SDLC port. You specify the topology when you configure SDLC on the synchronous circuit.

For more information on the Bay Networks SDLC implementation, see *Configuring SDLC Services.*

Integrated SDLC Conversion

Integrated SDLC conversion enables existing SDLC traffic to share a backbone network with LAN traffic without an intervening TCP/IP network. Traffic enters the DLSw router as SDLC and goes out the router as LLC2 over Token Ring or Ethernet. The destination endstation can reside on the Token Ring or Ethernet directly connected to that DLSw router. SRB can forward the traffic through the network to a destination host or endstation. In this network, the local router performs the SDLC conversion, and forwards the traffic across the network to the host (Figure 1-5).

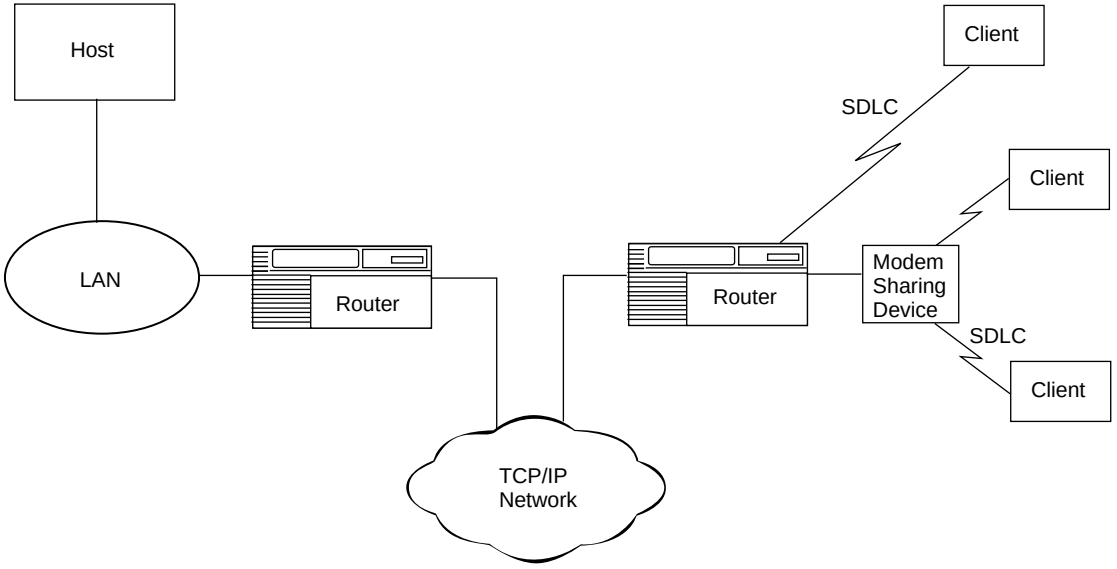


Figure 1-5. SDLC Conversion in a Single-Switch Configuration

In Figure 1-5, the SDLC clients appear to both the network and the Token Ring LAN-attached host as if they were natively LAN-attached.

Figure 1-6 illustrates a DLSw dual switch-to-switch network with SDLC clients using DLSw services at the local router to communicate over TCP/IP with a remote host attached to a Token Ring LAN.

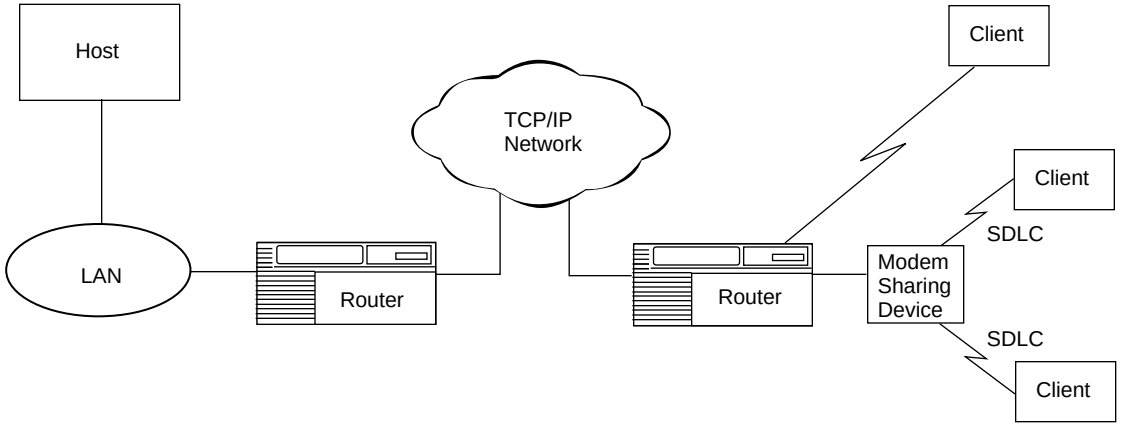


Figure 1-6. SDLC Conversion in a Dual Switch-to-Switch Configuration

In this example, the local router performs the following operations:

- Terminates the SDLC sessions
- Converts the SDLC traffic to DLSw Switch-to-Switch Protocol (SSP) format for TCP/IP routing
- Forwards the traffic to the remote router

The DLSw remote router does the following:

- Converts the traffic to the appropriate format
- Sends the traffic to the destination host

In Figure 1-6, the SDLC clients appear to the network and to the Token Ring LAN-attached host as if they were natively attached LAN devices.

In both single and dual switch-to-switch networks, you must map the addresses of the SDLC devices to Token Ring/802.5 addresses. To map the addresses, you configure the SDLC devices as local devices, enabling them to appear to the network as natively attached LAN devices. Chapter 5 describes how to configure local devices.

Refer to *Configuring SDLC Services* for information on configuring and tuning SDLC on a Bay Networks router.

Frame Relay Support

Bay Networks routers support LLC2 routed over Frame Relay (also known as native SNA over Frame Relay) based on RFC 1490. RFC 1490 describes an encapsulation method for carrying internetwork traffic over a Frame Relay backbone. This implementation of LLC2 also complies with the Frame Relay Forum "Protocol Encapsulation over Frame Relay Implementation Agreements," which (1) defines how routed SNA traffic traverses a Frame Relay network and (2) adds RFC 1490 support for Frame Relay to DLSw and APPN.

LLC2 over Frame Relay allows native SNA traffic (originating from SDLC, LAN- or WAN-attached devices) to communicate over public or private Frame Relay networks directly with IBM 3745 or 3746 communications controllers. Devices can communicate with intermediate routing nodes or in a single-switch configuration function as a Frame Relay Access Device (FRAD).

Figure 1-7 illustrates the connection of a host through a Frame Relay network, in a configuration with multiprotocol traffic to other locations.

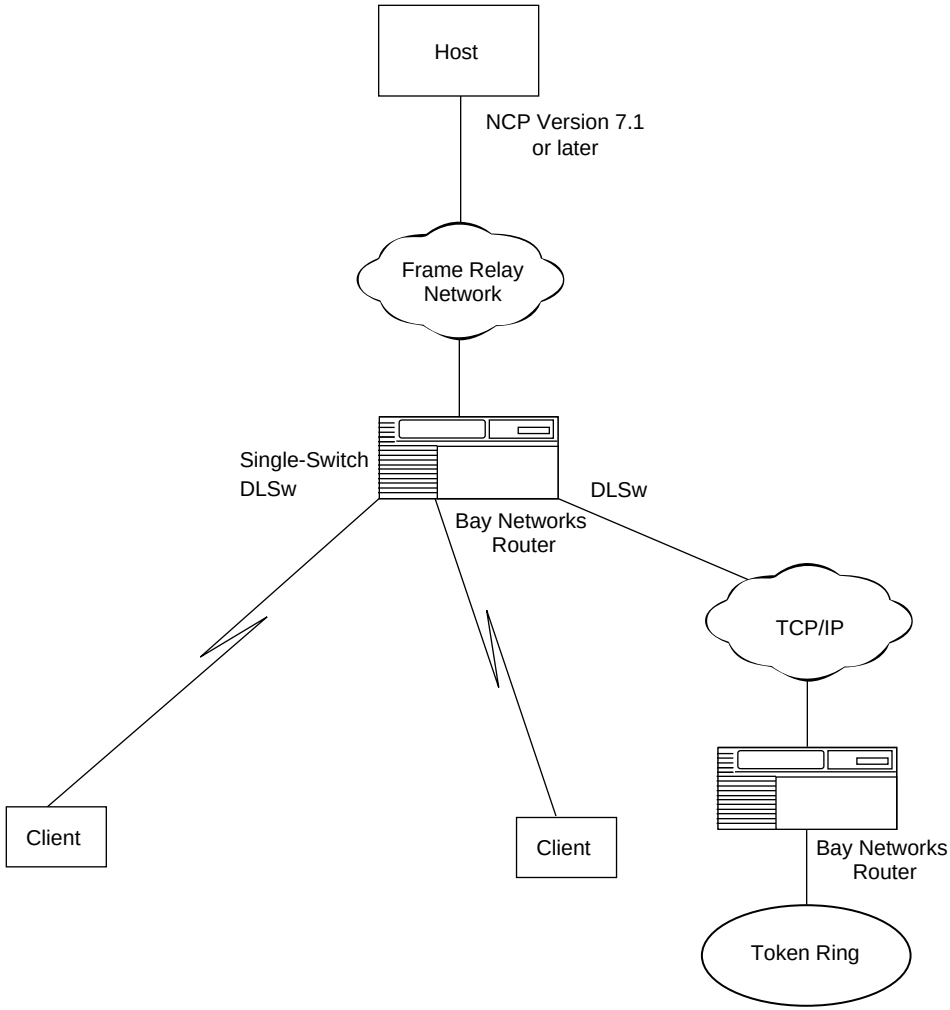


Figure 1-7. Sample Frame Relay Network

For more information on LLC2 over Frame Relay, refer to *Configuring LLC Services*.

DLSw Filtering

Bay Networks provides three filtering mechanisms that affect DLSw traffic:

- Inbound traffic filters
- DLSw prioritization
- Protocol prioritization

Inbound Traffic Filters

DLSw supports inbound traffic filtering. You can establish filters associated with any remote DLSw TCP port. The filters allow the router to

- Drop a packet
- Log a packet
- Forward a packet to a specific address (outbound to TCP)

For DLSw services:

- Actions other than LOG apply only to broadcast frames sent over the TCP/IP network.

For more information on how to access and configure traffic filters for DLSw services, refer to *Configuring Traffic Filters and Protocol Prioritization*.

DLSw Prioritization

DLSw prioritization allows you to prioritize traffic within DLSw based on predefined or user-defined fields. Examples of DLSw prioritization criteria include

- Source and destination SAP; this field can be used to assign NetBIOS traffic (SAP 0xF0) to a lower priority than SNA traffic.
- Source and destination MAC address; this can be used to provide host bound traffic preference over other traffic
- Any field in the SNA Transmission Header (TH) and Response/Request Header (RH); this can be used to provide Class Of Service (COS) priority preference

You can also prioritize traffic based on any values within the headers and data packets.

For detailed information about DLSw prioritization, refer to Chapter 6, “Using DLSw Prioritization.”

Protocol Prioritization

You can use protocol prioritization to transmit DLSw traffic before other traffic on an individual synchronous line interface. This is done by creating a filter, as follows:

- Criteria = TCP source port
- Range = 2065 - 2067
- Action = high queue

This ensures that SNA and NetBIOS traffic receive preference on the network. For more information on how to access and configure traffic filters for DLSw services, refer to Chapter 6, “Using DLSw Prioritization.”

DLSw and Related Protocols

DLSw uses the services of lower layer subsystems, depending on the type of interface being configured and the services required. Related subsystems include

- Physical interface: Token Ring, Ethernet, WAN, FDDI, etc.
- Transport services: Source Route Bridging, Transparent Bridging, Frame Relay, etc.
- Data Link Control services: LLC2, SDLC
- TCP/IP services (dual switch only)

For More Information about DLSw

The following publications provide more detailed technical information related to DLSw services:

- Dixon, Roy C., and Kushi, David M. *Data Link Switching: Switch-to-Switch Protocol, RFC 1434*, March 1993.
- IBM Corporation. *NetBIOS Frames Protocol, IBM Local Area Technical Reference, SC30-3383-03*, December 1990.
- International Standards Organization. *ISO 8802-2/IEEE Std 802.2 International Standard, Information Processing Systems, Local Area Networks, Part 2: Logical Link Control*, December 31, 1989.
- International Standards Organization. *ISO/IEC DIS 10038 DAM 2, MAC Bridging, Source Routing Supplement*, December 1991.
- Wellfleet Communications. *Integrating SNA & Multiprotocol LAN Networks, A Complete Guide*, March 1993.

Chapter 2
DLSw Implementation Notes

This chapter provides information on DLSw configurations, support protocols, and performance when configuring and customizing DLSw services on your network. It includes

- Source route bridge topologies
- Parallel data paths
- Multiple DLSw peers on a LAN
- DLSw and bridging services
- Memory requirements
- TCP considerations
- Flow control
- Performance

Source Route Bridge Topologies

This section describes how to count LAN and bridge elements along any DLSw connection path that passes through source-route-bridge (SRB) LANs (such as Token Ring/802.5) on either side of the TCP/IP network.

The physical elements in this path are the SRB LANs and the bridges between LANs. The logical elements (implemented in router software) are the IP Virtual Ring, the internal LANs, and the DLSw bridges. You must count all LAN and bridge elements in a path to avoid exceeding

- The number of SRB LAN and bridge elements allowed in a source routing network
- The number of SRB LAN and bridge elements allowed along a DLSw connection path that includes SRB segments

Counting SRB LANs and Bridges

A standard source routing network can include up to eight SRB LANs linked by seven bridges (Figure 2-1).

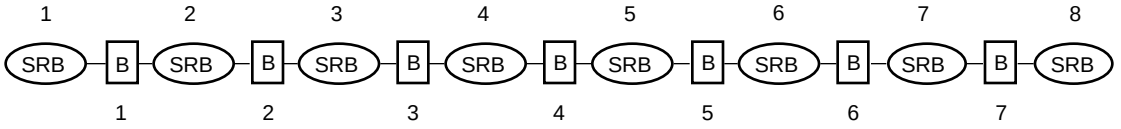


Figure 2-1. Maximum Ring and Bridge Hop Counts in a Source Routing Network

The term *source routing segment* refers to a linked series of rings and bridges attached to your network (Figure 2-2).

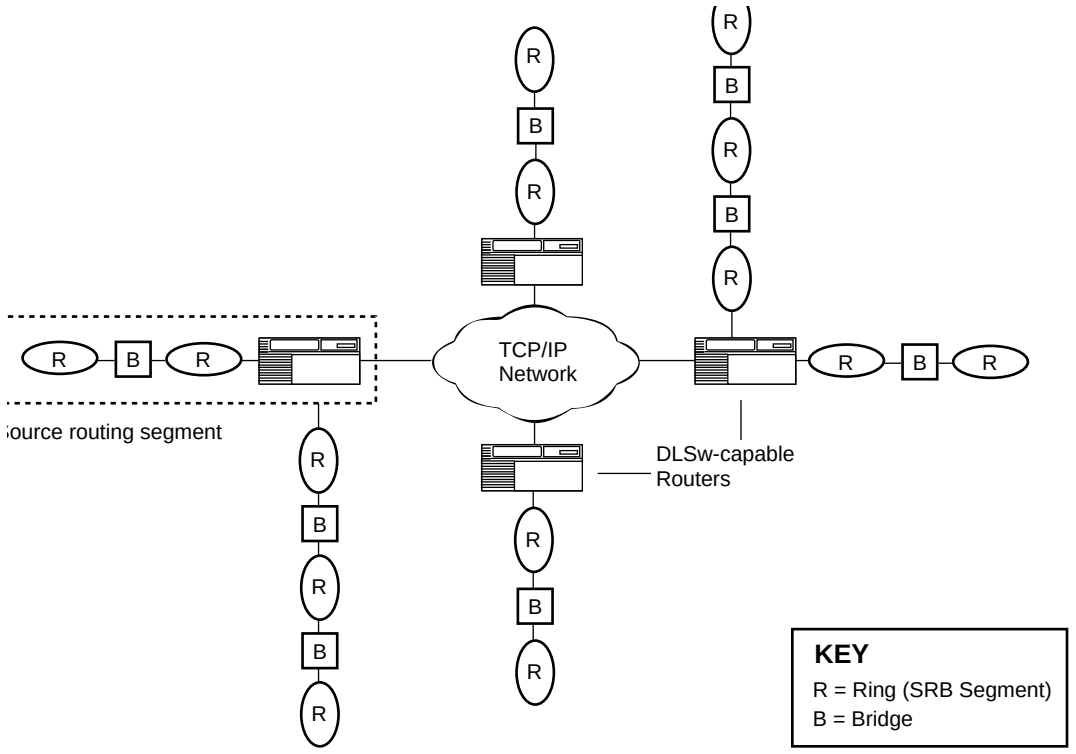


Figure 2-2. DLSw-Capable Routers on an IP Backbone

Counting the IP Virtual Ring

The DLSw peers at the periphery of a TCP/IP network collectively use an *IP virtual ring*, which provides compatibility with LAN requirements (Figure 2-3).

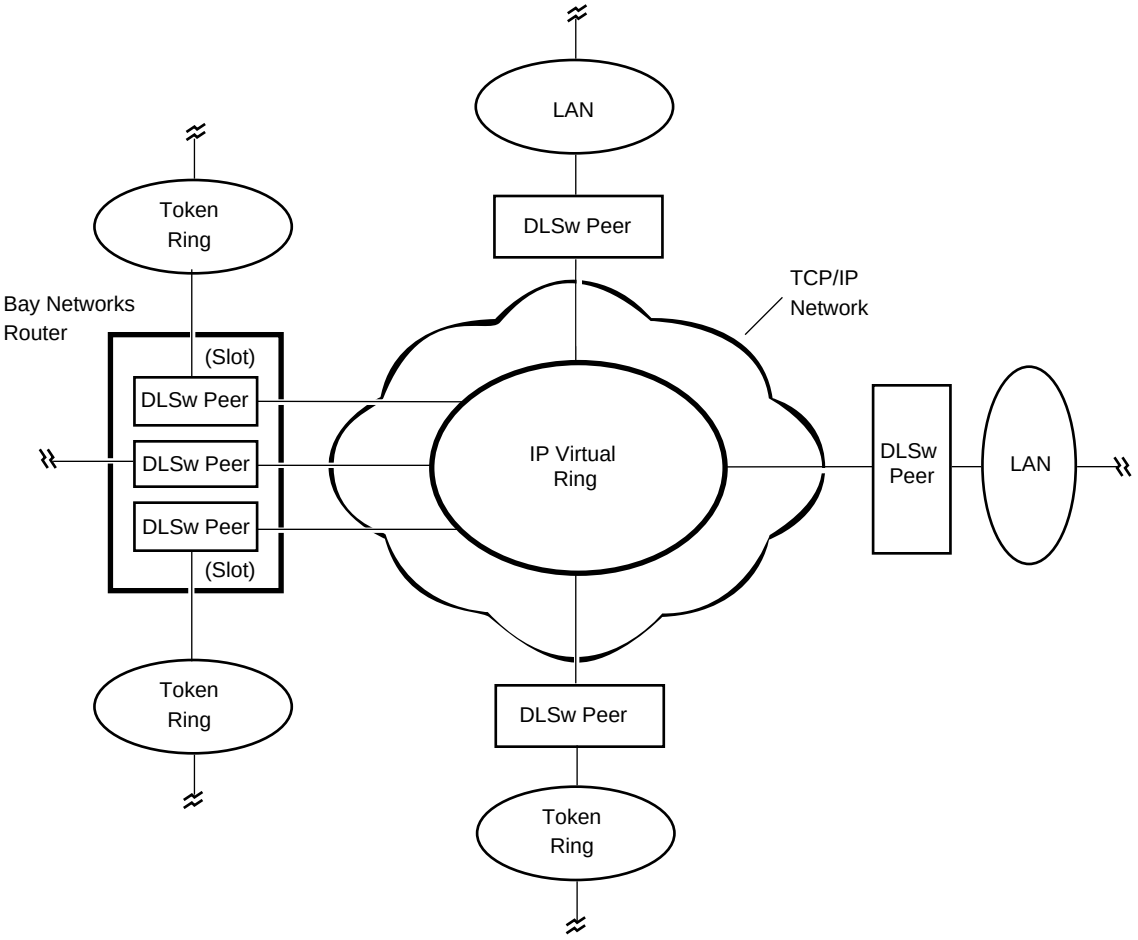


Figure 2-3. DLSw Peers Using an IP Virtual Ring

NetBIOS and SNA systems on a LAN attached to a DLSw peer perceive the IP virtual ring only as a physical boundary (the last ring) on that LAN or source routing segment.

You must count the IP virtual ring when you determine the number of ring and bridge elements in each source routing segment connected to a DLSw peer.

Just as each physical Token Ring in a source routing network has an associated Ring ID, the IP virtual ring also has a *Virtual Ring ID*. You enter the IP virtual ring ID with the IP Virtual Ring parameter.

The virtual ring also has an associated Maximum Transmission Unit (MTU) size. The Virtual Ring MTU parameter specifies a maximum size for frames sent from local systems to systems on remote source routing networks. Use as a value for the MTU the *smallest* frame size supported on any remote source routing segment in your network.

You can access and edit the IP Virtual Ring and Virtual Ring MTU parameters through the DLSw Global Parameters window.

Note: *Site Manager requires you to enter values for the IP Virtual Ring and Virtual Ring MTU parameters, even if your network only includes Ethernet/802.3 circuits configured for access to DLSw services.*

Count the IP virtual ring as one ring in each source routing segment attached to your TCP/IP network. You count the IP virtual ring first rather than last, to avoid configuring source routing segments that already contain more than eight ring elements (Figure 2-4).

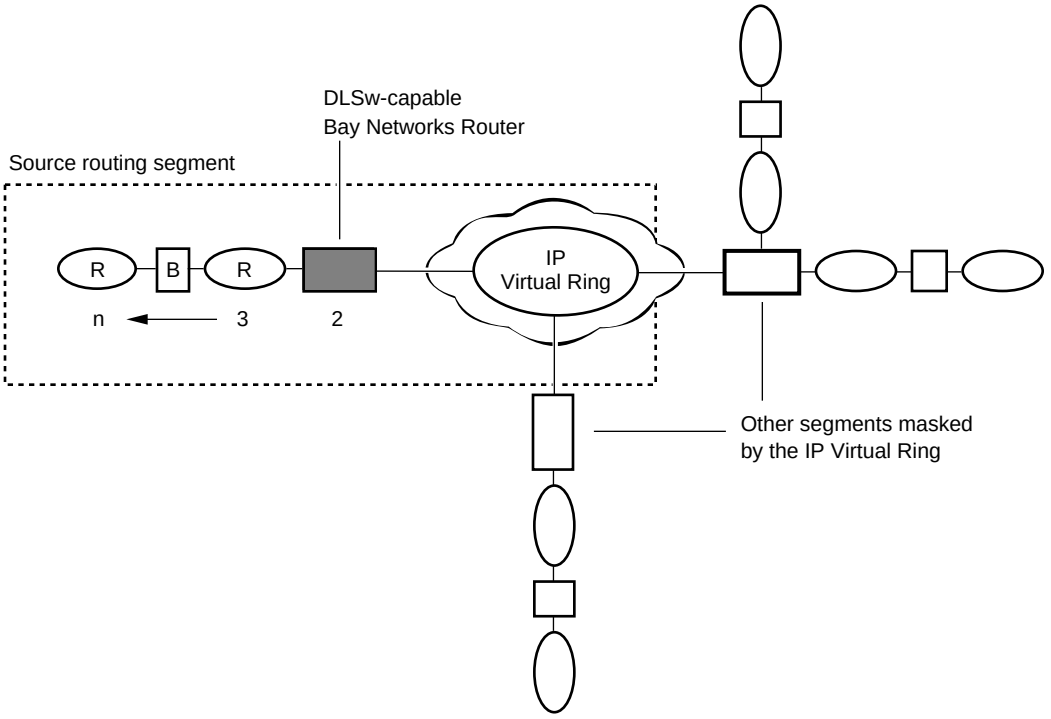


Figure 2-4. Counting the IP Virtual Ring

Counting the Internal LAN

Each DLSw-capable Bay Networks router between an SRB LAN and the TCP/IP network implements an internal LAN in the source routing bridge software (Figure 2-5).

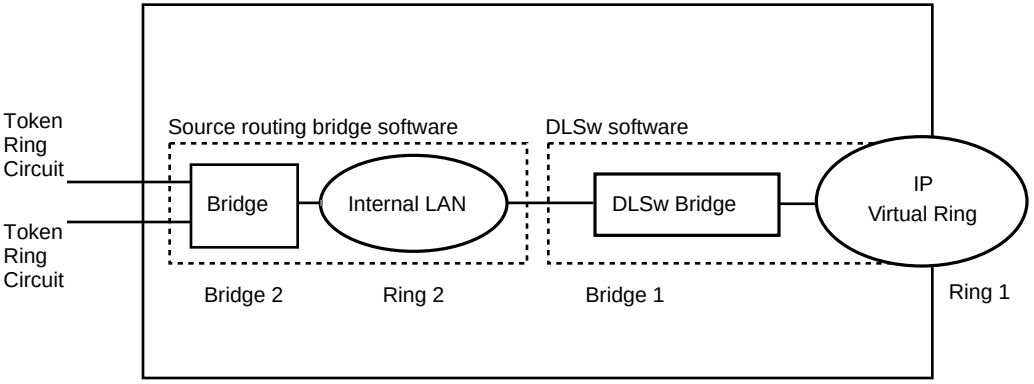


Figure 2-5. Router Logical Considerations for DLSw Support

The internal LAN is not an actual network, but you must account for it in topology calculations for SRB environments. The internal LAN also has an associated ID that you enter when you configure the source routing bridge global parameters for DLSw operation.

Refer to *Configuring Routers* or *Configuring Bridging Services* for more information on the internal LAN ID.

Count the internal LAN only once per source routing segment. (Ensure that the Group LAN ID is the same for all Bay Networks routers in the same source routing segment.)

Counting the DLSw Bridge

Each DLSw peer in your network implements a DLSw bridge between the internal LAN and the IP virtual ring. (Refer to Figure 2-5.) The DLSw bridge is part of the router software, not an actual bridge. You must, however, *count this as one bridge in a source routing segment.*

Computing a DLSw Connection Path

For SRB LAN environments, the longest DLSw connection path can include up to 15 SRB LANs and 14 bridge elements. Some of these elements are physical, others are logical (implemented in software).

For information on SRB LAN and bridge elements to count in other than Bay Networks DLSw-capable nodes, see the appropriate manufacturer's user documentation.

Figure 2-6 shows an end-to-end path that traverses two Token Ring LANs and an intervening TCP/IP network. A DLSw-capable Bay Networks router connects each Token Ring LAN to the periphery of the TCP/IP network. The path shown in Figure 2-6 contains the maximum of 15 ring elements and 14 bridge elements. (Note that although the figure shows Token Ring LANs, DLSw supports all other SRB LANs.)

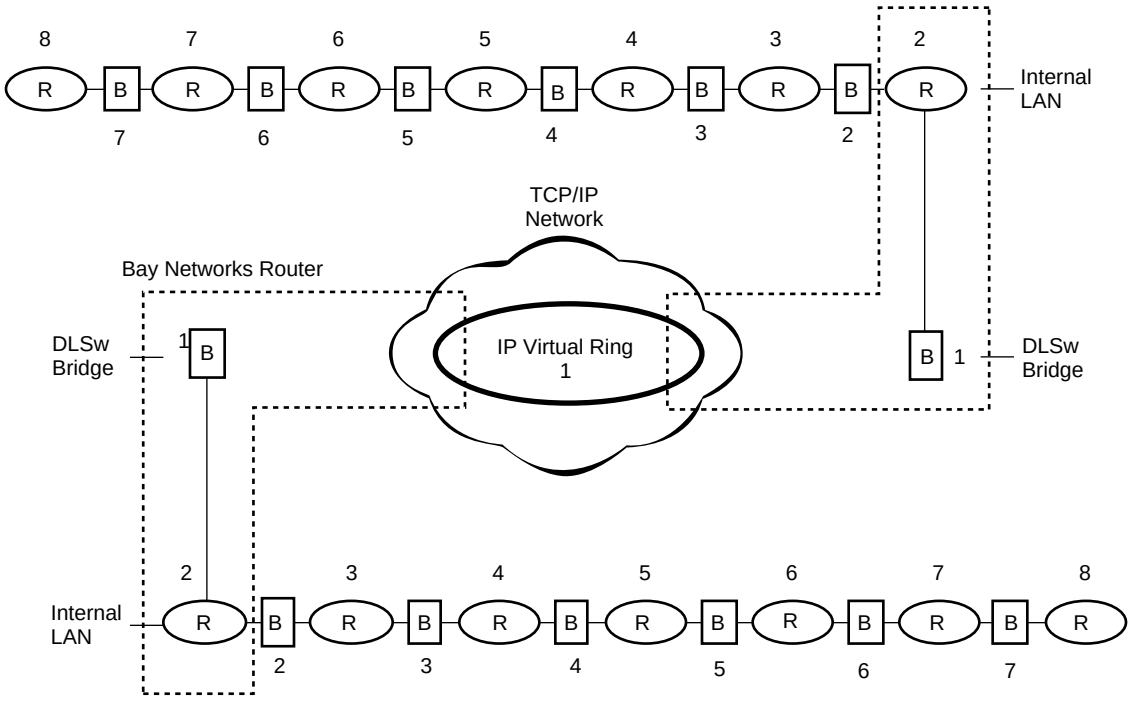


Figure 2-6. End-to-End Path in a DLSw-capable Token Ring/802.5 Network

For mixed topologies (SRB and non-SRB LANs), an end-to-end connection path includes an SRB and a non-SRB LAN. In such cases, do not exceed the maximum number of SRB LAN and bridge elements allowed on the SRB LAN side of the connection path.

Parallel Data Paths

If a valid bridging path already exists between two LANs, *do not* configure a parallel DLSw connection path between the same two LANs (Figures 2-7 and 2-8). Parallel data paths allow frames to traverse the LANs twice which, in turn, may confuse systems on the associated LAN segments.

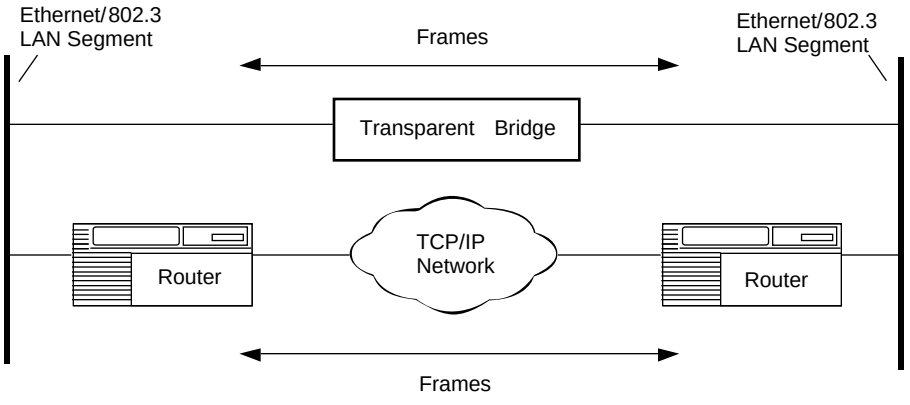


Figure 2-7. DLSw Services in Parallel with a Transparent Bridge

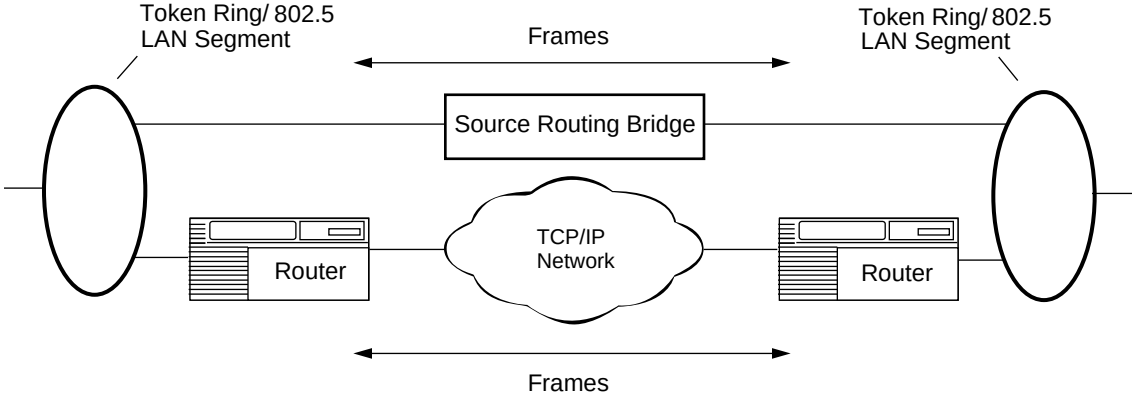


Figure 2-8. DLSw Services in Parallel with a Source Routing Bridge

Multiple DLSw Peers on a LAN

You can configure two or more DLSw nodes on the same SRB LAN. With this configuration, each DLSw peer reaches a different set of remote NetBIOS and SNA systems. In this case,

- Do *not* define a TCP connection between these Data Link Switches.
- Assign the same Virtual Ring IDs to each peer.

Taking these precautions prevents frames sent by one DLSw node from propagating through the other DLSw node on the same SRB LAN.

Note: *Do not configure multiple Data Link Switches on an Ethernet/802.3 LAN. Ethernet/802.3 LANs do not support loop prevention through source routing.*

DLSw and Bridging Services

This section presents the different types of bridging services that coexist on a circuit with DLSw, and explains any differences in TEST or explorer frame handling on these circuits. This information is useful when you examine traffic on LANs locally attached to the router.

DLSw on an SRB Circuit

On an SRB circuit with DLSw services enabled (Figure 2-9), the following rules apply:

- Upon receiving an explorer frame that contains a DLSw-specific destination SAP address, DLSw and SRB attempt concurrently to locate the requested program entity.
  - — DLSw searches the network for a route to the target system by forwarding the packet to all local DLSw interfaces and all known remote DLSw routers.
  - — SRB looks for a bridged path to the target system using standard source route bridge broadcasts.

- DLSw or SRB, whichever receives a response first, takes precedence. The slower subsystem ceases any further attempts to support a connection to the target program.

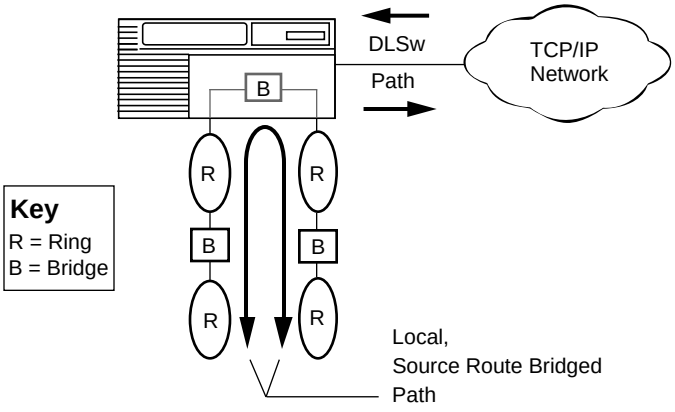


Figure 2-9. DLSw and Source Route Bridging on SRB Circuits

DLSw on an Ethernet/802.3 Circuit

The router supports DLSw configured on an Ethernet/802.3 circuit. The DLSw software provides bridging services between Ethernet/802.3 LAN segments locally attached to the same router.

The DLSw interface takes precedence over the transparent bridge interface whenever the destination SAP address identified in a TEST frame received from the local circuit already exists in the router's DLSw configuration. In this case, only the DLSw interface

- Captures the locally received TEST frame
- Attempts to locate the destination SAP address specified in that frame

The transparent bridge interface on the same circuit with DLSw never sees TEST frames that contain destination SAP addresses intended for DLSw (Figure 2-10). However, SAP addresses intended for DLSw can be passed from one local Ethernet interface to another through the DLSw software. Therefore, non-DLSw SAPs will be transparently bridged between transparent bridge interfaces while DLSw SAPs will be forwarded between interfaces by DLSw.

You configure transparent bridge services independent of DLSw services on the router, as appropriate for the topology of your network.

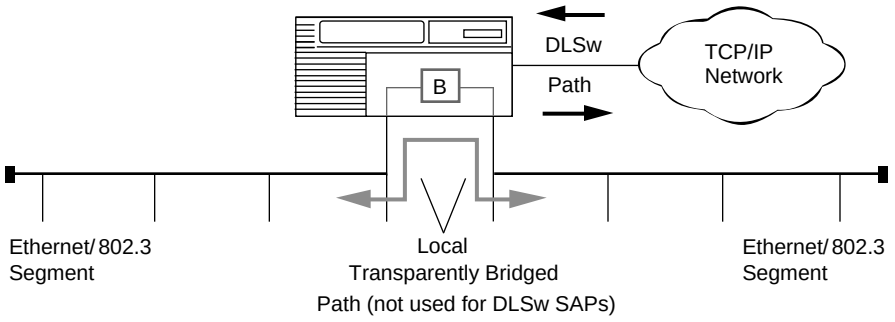


Figure 2-10. DLSw and Transparent Bridging on Ethernet/802.3 Circuits

DLSw with Translation Bridge

The router supports DLSw and translation bridge services on an Ethernet/802.3 circuit (Figure 2-11). (You configure translation bridge services independent of DLSw services on the router, as appropriate for the topology of your network.)

To an end-user system on an SRB circuit, the translation bridge looks like a source routing bridge. To an end-user system on an Ethernet/802.3 circuit, the translating bridge looks like a transparent bridge.

.

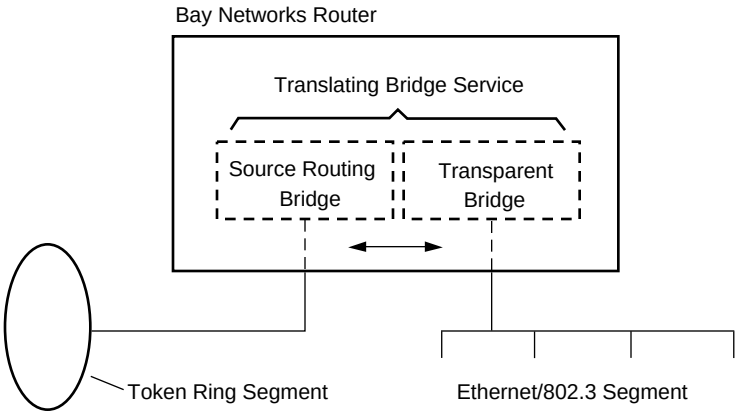


Figure 2-11. Translation Bridge Services

The translation bridge service

- Supports communication between systems on SRB and Ethernet/802.3 segments locally attached to the same router
- Maps between SRB and Ethernet/802.3 framing requirements

Memory Requirements

DLSw provides buffering of LLC2 packets in single switch mode, and additional buffering of TCP packets in dual switch mode. Therefore, DLSw can use a significant amount of memory.

To limit the memory consumption, Bay Networks provides several mechanisms, including

- LLC2 Max Links parameter, allowing the network administrator to limit the number of LLC2 stations *per interface*. Refer to *Configuring LLC Services*.
- DLSw Max Slot Sessions parameter, allowing the network administrator to limit the number of LLC2 stations *per slot*. See Chapter 5 for instructions on accessing and editing the Max Slot Sessions (DLSw global) parameter.
- Technician Interface commands, allowing the user to limit the total memory used by DLSw.

For more information on DLSw memory usage, contact Bay Networks Technical Response Center.

TCP Considerations

TCP timers allow you to configure DLSw to periodically give TCP data to transmit if a connection is inactive for a period of time. The mechanism by which TCP determines a lost connection (either a failed link with no rerouting possible, or the remote router is unavailable) is based on TCP attempts to deliver this data. If TCP does not receive an acknowledgment after a series of retries, it declares the connection down and informs DLSw. DLSw then manages the currently active sessions.

There are two main configuration parameters associated with DLSw timers:

- DLSw Keepalive Time
- TCP Max Retransmission Timeout

Configuring TCP Services describes the Max Retransmission Timeout parameter. This section describes the Keepalive Time and the Max Retransmission Timeout parameters.

DLSw Keepalive Time

The DLSw Keepalive Time parameter ensures that the TCP connection to a remote router is active. You enable the parameter by specifying a nonzero value. The Keepalive Time setting determines when to send data into the TCP pipe. Since only one packet is sufficient to initiate the TCP retransmission procedure, short intervals (less than 30 seconds) will use additional memory and resources unnecessarily. Low values (such as 1 second) do not significantly decrease notification time, but significantly increase CPU and WAN bandwidth utilization because each “keepalive” sends data into the TCP connection, awaiting acknowledgment by the remote router.

In busy networks, the DLSw keepalive is not necessary. Frequent traffic for TCP transmission performs the same function as a keepalive setting. For example, frequent NetBIOS broadcast traffic functions as a TCP keepalive.

The Keepalive Time parameter appears on the Edit DLSw Global Parameter window.

TCP Max Retransmission Timeout

The TCP Max Retransmission Timeout parameter setting determines the maximum time between successive retransmissions. TCP performs calculations that increase the time between data retransmissions to minimize network loading during peak periods when there is an increased risk of lost data. TCP starts a minimum retransmission time before increasing to the Max Retransmission Timeout setting with successive retransmissions. Decreasing the Max Retransmission Timeout decreases the notification time by reducing the time between intervals. This also slows network traffic in congested, connected networks.

In large networks with many routers, quick notification of a failed router or link is necessary. However, when some routers use a low Max Retransmission Timeout parameter setting, other routers using the default setting may cause inconsistent results. This means that some of the routers time out and report the lost TCP connections quickly, while other routers using the default setting may take up to 20 minutes.

The Max Retransmission Timeout default setting is 240000 ms (4 minutes), yielding a default time for learning of a lost TCP connection to approximately 20 minutes. Refer to *Configuring TCP Services* for information on editing the Max Retransmission Timeout parameter setting.

Flow Control

DLSw uses the following two flow control mechanisms to provide reliable end-to-end delivery of packets:

- LLC2 flow control
- TCP flow control

TCP and LLC2 continue to assert flow control until congestion clears on a given TCP connection.

The default settings for system parameters relevant to LLC2 and TCP flow control are suitable for the majority of your DLSw service requirements.

LLC2 Flow Control

The LLC2 protocol interface provides a bidirectional window mechanism and a SAP credit allocation mechanism that together manage flow control on individual LLC2 connections between the router and LAN-attached SNA or NetBIOS systems.

The SAP window attempts to limit the number of outstanding frames queued for transmission to a remote endstation from a local endstation at this SAP address, as follows.

1. As frames are sent by the local endstation but not yet acknowledged by the remote endstation, a counter on the remote DLSw switch increments.
2. When this counter reaches half the value specified in the SAP Window parameter, the remote DLSw switch sends a flow control indication back to the local DLSw switch.
3. The local DLSw switch sends RNRs (Receiver Not Ready) to the local endstation to control the flow of the session.
4. As frames are acknowledged by the remote endstation, the counter on the remote DLSw switch decrements.
5. After all outstanding frames have been acknowledged by the remote endstation, the remote DLSw switch sends an end-flow-control indication back to the local DLSw switch.
6. The local DLSw switch then sends RR (Receiver Ready) to the local endstation, thereby allowing it to send more frames.

TCP Flow Control

Each pair of TCP connections between DLSw peers carries data from many LLC2 sessions. When congestion occurs on the TCP/IP network between DLSw peers, TCP

- Reduces or closes its transmit window
- Signals the local and remote LLC2 interfaces to assert flow control on any LLC2 connections associated with the congested TCP connections

Performance

In a DLSw configuration that includes a single IP virtual ring, the operation of three connection-oriented protocol components (two LLC2 and one TCP) in the data path between endstations may affect end-to-end performance. Performance delays increase for DLSw configurations that include more than one IP virtual ring in any end-to-end connection path. (For more information on DLSw configurations that include multiple IP virtual rings in an end-to-end connection path, contact the Bay Networks Technical Response Center.)

You can make determinations of DLSw latency, based on your experience with specific SNA and NetBIOS applications. Consider also the inherent latency of the physical data links that interconnect each pair of DLSw peers.

DLSw Packaging

In DLSw dual switch configurations, packaging allows multiple DLSw frames (consisting of user data and the DLSw SSP header) to be placed into a single TCP/IP frame. This provides two performance benefits:

- Reduces the number of TCP/IP encapsulation program executions. This results in fewer router cycles when processing DLSw information.
- Reduces the amount of TCP/IP overhead per DLSw frame. Instead of 52 bytes of overhead per information frame (32 for TCP, 20 for IP), a single TCP/IP package carries multiple frames.

With DLSw packaging, a packet may be delayed for a short period while the router waits to see whether there are any more packets routed to the same destination peer. This delay may increase network latency. However, the performance benefits increase the number of packets that can be delivered across the network, increasing response time. DLSw packaging is important for networks with many LAN/WAN segments and for networks with slow WAN links.

For information on configuring DLSw packaging parameters, refer to Chapter 5.

Chapter 3
DLSw Configuration Overview

This chapter provides general information about configuring DLSw on Bay Networks routers, including

- DLSw session setup overview
- Site Manager roadmaps to configuring DLSw
- Configuration objects for single switch DLSw
- Configuration objects for dual switch DLSw
- Configuration objects for SDLC
- Optional configuration objects

DLSw Session Setup Overview

Before configuring DLSw, you should be familiar with how DLSw establishes sessions between network endpoints. To establish SNA or NetBIOS sessions between endpoints (devices), Bay Networks routers with DLSw enabled execute the following sequence of events:

- Upon receiving a TEST (POLL) or similar frame from an attached endstation, the receiving slot performs the following:
  - — Forwards the packet to all other slots defined in the DLSw Slot Table.
  - — Converts the TEST (POLL) frame into an SSP CANUREACH command.
  - — Searches the appropriate cache to determine if the remote location is known. If the remote location is already in the cache, the CANUREACH is forwarded only to this remote location. If the remote loccation is not in the cache, DLSw forwards the CANUREACH to all remote routers specified in the DLSw Peer IP Table, if this table exists.

- Upon receiving a CANUREACH frame, a DLSw slot:
  - — Forwards the frame to all other slots defined in this router's DLSw Slot Table.
  - — Converts the CANUREACH frame back to a TEST (POLL) frame.
  - — Forwards the TEST (POLL) frame to all interfaces on this slot which have DLSw enabled.
- If the destination device resides on an attached LAN, then this device responds by broadcasting a TEST (RESPONSE) message. Upon receiving this response, the remote router:
  - — Caches the MAC address (for SNA) or name (for NetBIOS) in the appropriate table on the router.
  - — Converts the TEST (RESPONSE) packet into a DLSw ICANREACH frame.
  - — Forwards the ICANREACH to the originating data link switch (router).
- Upon receiving the ICANREACH, the originating router:
  - — Caches the MAC address or NetBIOS name, and identity of the remote router in the appropriate table on the router.
  - — Converts the ICANREACH back to a TEST (RESPONSE) frame.
  - — Forwards the packet to the originating workstation.

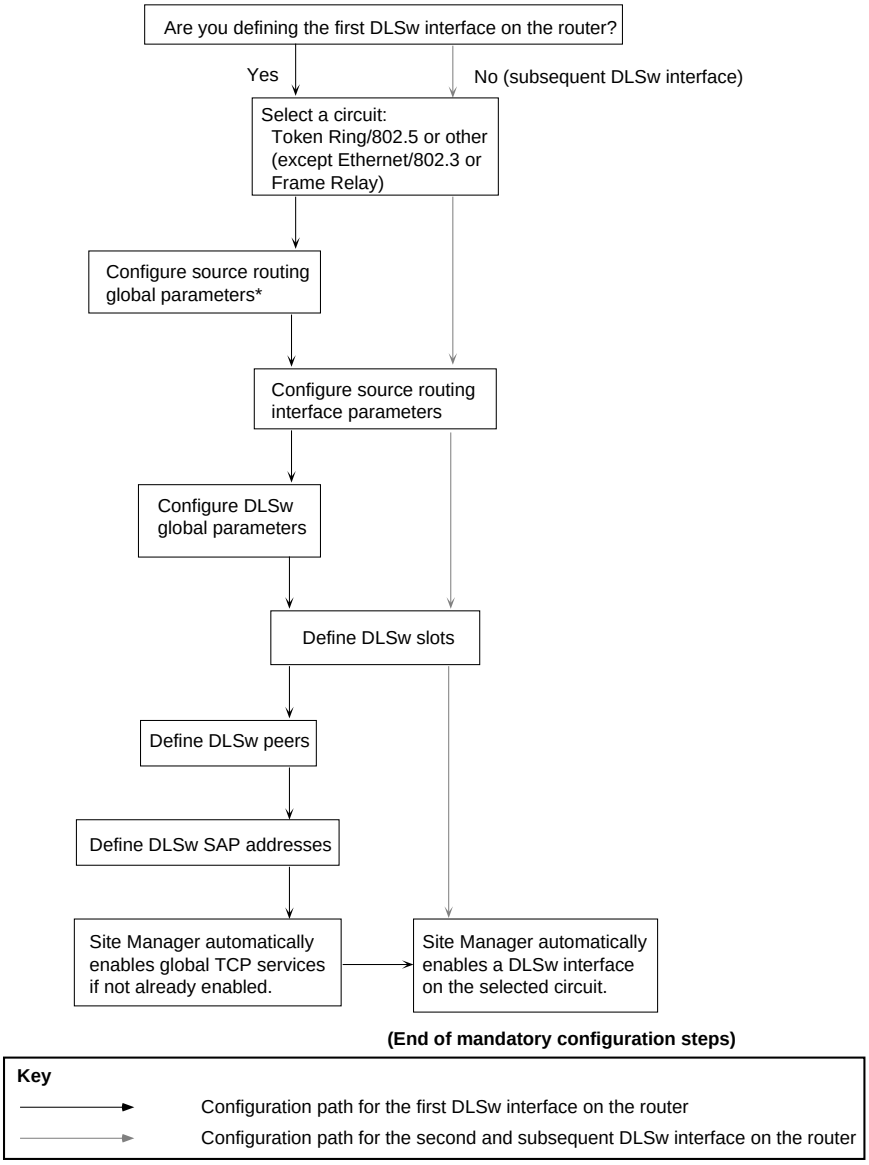
At completion, all routers and endstations can forward SNA and NetBIOS packets appropriately, creating a logical session between endpoints.

Each slot on a Bay Networks running DLSw functions as an independent Data Link Switch. The network administrator controls the packets forwarded to DLSw by specifying the appropriate SAPs in the DLSw SAP Table.

Site Manager Roadmaps to Configuring DLSw

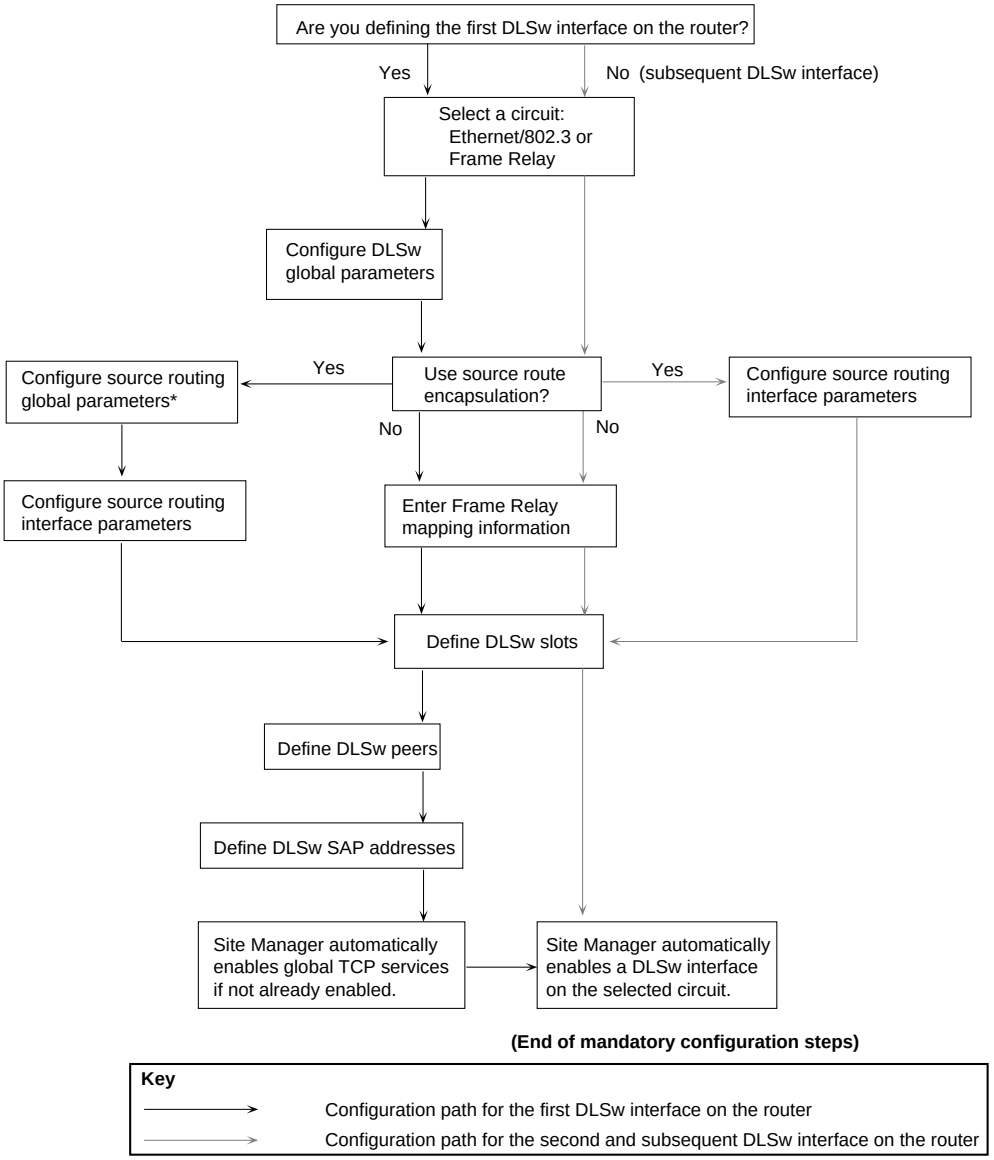
Figures 3-1 and 3-2 illustrate roadmaps to configuring and enabling DLSw on a Bay Networks router. The roadmap you use depends on the specific type of interface on which you are configuring DLSw.

Figure 3-1 illustrates the steps for configuring DLSw on Token Ring or other source route bridge networks. Figure 3-2 illustrates the steps for configuring DLSw on Ethernet/802.3 or Frame Relay.



* If you already configured source routing on your router, Site Manager does not prompt you to configure source routing global parameters during the DLSw configuration sequence.

Figure 3-1. DLSw Configuration Sequence for Token Ring/802.5 or Other Source Route Bridge Networks


Are you defining the first DLSw interface on the router?
Yes
No (subsequent DLSw interface)
Select a circuit: Ethernet/802.3 or Frame Relay
Configure DLSw global parameters
Use source route encapsulation?
Yes
Configure source routing global parameters*
Yes
Configure source routing interface parameters
No
No
Configure source routing interface parameters
Enter Frame Relay mapping information
Define DLSw slots
Define DLSw peers
Define DLSw SAP addresses
Site Manager automatically enables global TCP services if not already enabled.
Site Manager automatically enables a DLSw interface on the selected circuit.
(End of mandatory configuration steps)
Key
Configuration path for the first DLSw interface on the router
Configuration path for the second and subsequent DLSw interface on the router

* If you already configured source routing on your router, Site Manager does not prompt you to configure source routing global parameters during the DLSw configuration sequence.

Figure 3-2. DLSw Configuration Sequence for Ethernet/802.3 or Frame Relay Network

Configuration Objects for Single Switch DLSw

This section describes the objects you define when you configure DLSw services on the router, specifically,

- DLSw SAPs
- DLSw slots

DLSw SAP Table

For DLSw services to be applied to a packet, you must define the packet's SAP to DLSw. Each router maintains an independent list of DLSw SAP addresses in a global DLSw SAP Table. Use the Configuration Manager to access and edit the DLSw SAP Table.

Each DLSw SAP Table entry has a unique hexadecimal value. The default SAP Table includes SAPs 00, 04, 08, and 0C (hexadecimal). This is sufficient for most SNA applications. To support NetBIOS, add SAP F0 to the SAP Table.

Figure 3-3 shows a sample network with three routers running DLSw. This network uses the following values in the SAP Tables:

- Router A, the central site router, supports both SNA and NetBIOS traffic. SNA session traffic uses SAP 04, and NetBIOS traffic uses F0. Additionally, SNA requires SAP 00 for session initiation. These hexadecimal values (00, 04, F0) must exist in the SAP Table.
- Router B, the remote site, supports NetBIOS traffic only. SAP F0 is the only required entry in the SAP Table.
- Router C, a regional site, supports SNA traffic only. In this example, SNA requires SAPs 00 and 04 in the SAP Table.

Note that SNA traffic can use other SAPs. Most SNA traffic uses SAP 04.

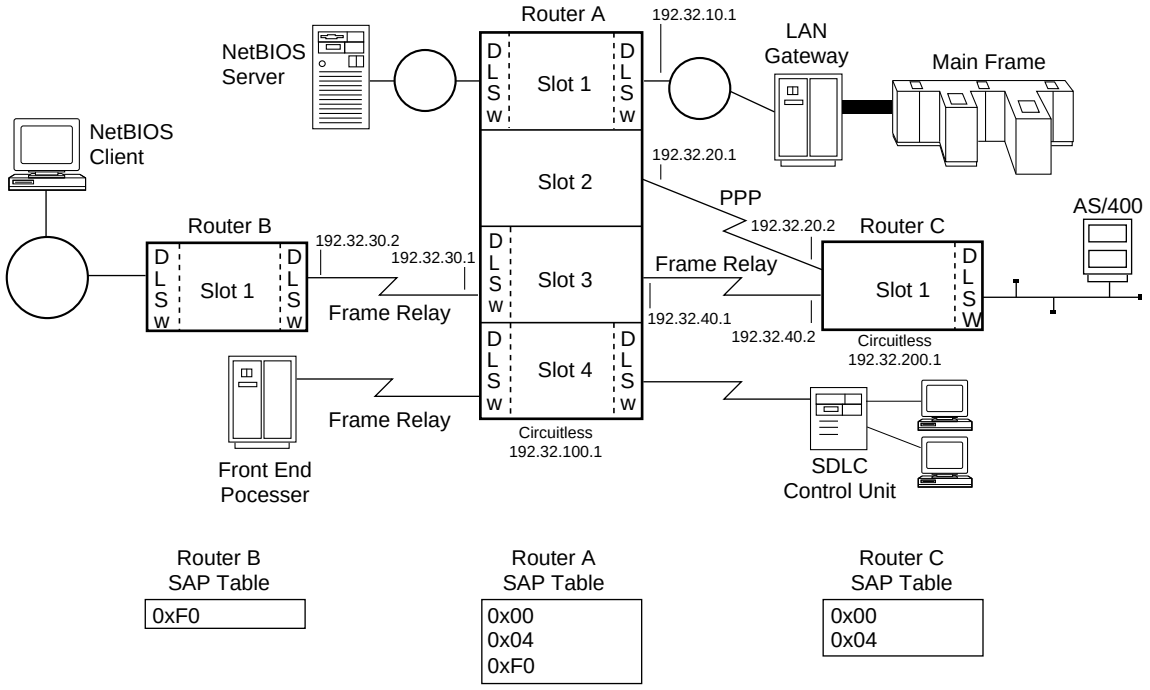


Figure 3-3. Sample Network with SAP Table Definitions

Refer to Chapter 5 for more information about accessing and editing the DLSw SAP Table.

DLSw Slot Table

Each slot on a Bay Networks router running DLSw acts as an independent data link switch. Each slot is identified by assigning a *unique* IP address for the slot. This mapping is done in the DLSw Slot Table. Each entry in the table consists of a DLSw slot number plus the address of the IP interface you allocate for that slot.

The router uses this IP address to establish the TCP sessions between peers in a DLSw network. Generally, the IP address that you select is either the circuitless IP address or the IP address of any interface on this slot. However, it is acceptable to use the IP address of any interface on any slot.

If a unique IP address is not available, you must perform one of the following tasks:

- For configurations that do not have as many physical IP interfaces as DLSw slots, add multiple IP addresses to a single physical interface. For example, you might want to do this in large SDLC configurations, since IP cannot be configured on SDLC interfaces. For more information on configuring multiple IP addresses, see *Configuring IP Services*.
- For single switch operation, enter any valid IP address that is available but not used in your network. This address should be on a unique IP subnet.

Note: *You can use the circuitless IP interface address for one (and only one) DLSw-capable slot. Using the circuitless IP interface allows TCP connections for DLSw services on that slot to be less dependent on the availability of specific physical circuits or data links. We recommend that you set the Keepalive Time parameter to a nonzero value when using the circuitless IP address. (For more information on the circuitless IP interface, refer to* Configuring IP Services.*)*

Figure 3-4 shows a sample network with three routers running DLSw. Although many options exist for the Slot Table, this network uses the following values in the Slot Tables:

- Router A, the central site router, has three slots running DLSw, as follows:
  - — For Slot 1, the circuitless IP address is used in the Slot Table to represent this slot. This provides the highest availability for Token Ring devices.
  - — For Slot 3, the IP address of the directly attached Frame Relay interface represents this slot in the Slot Table.
  - — For Slot 4, note that an IP address cannot be assigned to an SDLC interface, and no IP address is assigned to the Frame Relay interface. Instead, the IP address of a Token Ring interface on Slot 1 is used in the Slot Table. It is acceptable to use any other IP address existing on this router to represent this slot.
- Router B, a remote site connected to the central site using Frame Relay, is a single slot router running single switch DLSw. The IP address of the Frame Relay interface represents this slot in the Slot Table.

- Router C, a regional site connected to the central site using multiple links, is a single slot router running dual switch DLSw. The circuitless IP address represents this slot in the Slot Table.

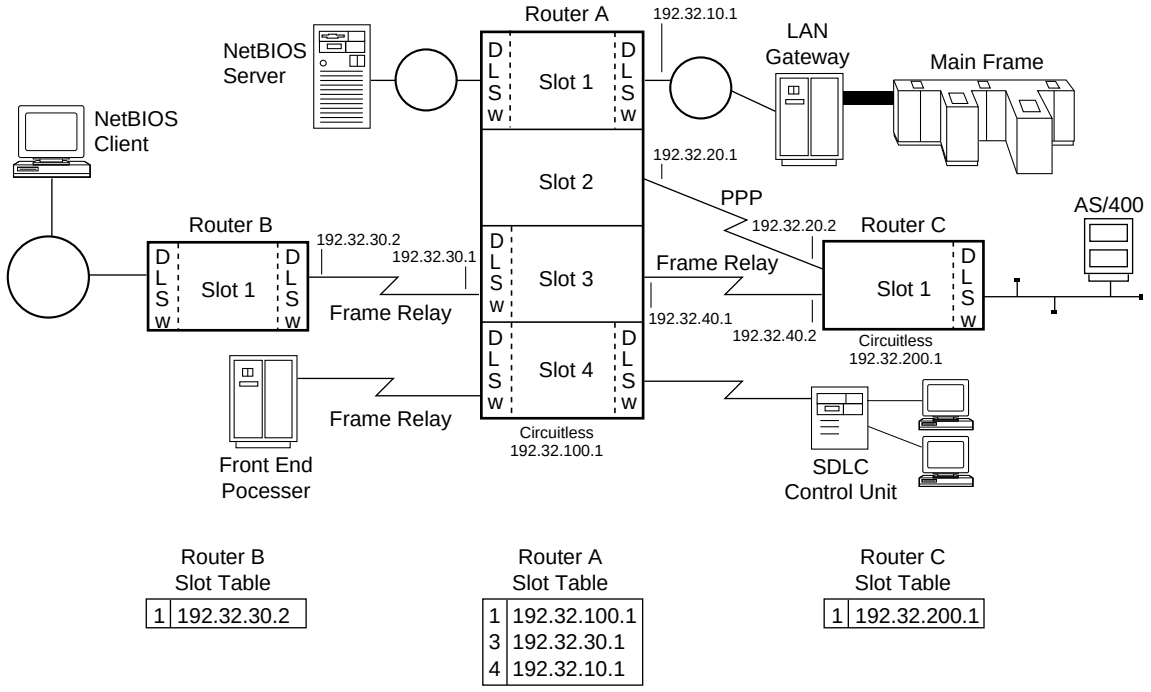


Figure 3-4. Sample Network with Slot Table Definitions

You enter slot information in the DLSw Slot IP Table during the initial configuration procedure. Refer to Chapter 5 for more information about accessing and editing the DLSw Slot IP Table.

Configuration Objects for Dual Switch DLSw

This section describes the objects you define when you configure DLSw dual switch services on the router, specifically DLSw peers.

DLSw Peer IP Table

Data Link Switches that connect to the same TCP/IP network are called *DLSw peers* on that network. On Bay Networks routers, each slot that you configure with DLSw services functions as an independent DLSw peer. Other vendors may offer RFC 1434-compliant products that support either single or multiple DLSw peers internally. For example, each IBM 6611 processor in your network serves as a single DLSw peer that you must define on the router.

TCP/IP sessions between DLSw peers are used to exchange information between devices attached to each peer. In each router, you can define a list of peers in remote routers with which a DLSw session can be initiated. These are called *configured peers*, and are defined in the DLSw Peer IP Table.

You can establish DLSw peer configurations that include only Bay Networks routers or a mix of Bay Networks routers, and other RFC 1434-compliant devices.

Configured Peers

A configured peer is a remote Data Link Switch (represented by an IP address) that is predefined in the local router. You define a configured peer by specifying its unique IP address in the Site Manager DLSw Peer IP Table.

IP addresses in the local router's Peer IP Table must also appear in the Slot Table of a remote router.

A configured peer can receive broadcast frames directly from DLSw peers in a local router.

The local router issues broadcast frames triggered by client demand for connection services. Responses to these broadcasts enable the local router to

- Identify DLSw peers that can reach the requested remote NetBIOS or SNA system
- Manage (open, restart, and close) TCP connections to the DLSw peer that can reach the requested SNA or NetBIOS system

Once a router knows that a DLSw peer can reach a specific system, the router can address frames directly to that peer and avoid unnecessary broadcast traffic on the TCP/IP network.

You typically define as configured peers

- One slot in each DLSw-capable remote Bay Networks router in your TCP/IP network to which broadcast traffic must be forwarded.
- Any other RFC 1434-compliant peer in your TCP/IP network.

You define each configured peer by its unique IP address on the TCP/IP network.

Once you initialize DLSw services, the local router establishes two TCP connections (one for transmitting, one for receiving) between each local DLSw-capable slot and every configured peer in the TCP/IP network. (Remote DLSw peers on the network follow the same procedure.) DLSw uses TCP ports 2065 and 2067.

Simplifying the Peer IP Table

Bay Networks provides two mechanisms for reducing the number of required entries in the DLSw Peer IP Table. These are

- Broadcast peers
- Unconfigured peers

Broadcast Peers

Any DLSw slot that receives a broadcast will forward that frame to all other DLSw slots in this same router. Therefore, it is not necessary to enter more than one peer (per remote router) into the Peer IP Table. The entry representing the remote router is the *broadcast peer* for that router.

Unconfigured Peers

A Bay Networks router running DLSw can respond to requests from remote routers to initiate DLSw sessions, even if the remote peer is not defined in the local router's Peer IP Table. Once a DLSw session is established to a remote slot, that slot is dynamically added to the list of known peers. Any remote DLSw peer that the router learns dynamically is an *unconfigured peer.* These peers are not listed in a router's Peer IP Table.

Unconfigured peers are supported only if the DLSw Reject Unconfigured Peers parameter is set to Accept.

Unconfigured peers normally do not receive broadcast frames from another router. However, unconfigured peers on a remote Bay Networks router can both receive and respond to broadcast frames that the configured peer in that router forwards internally.

When a local DLSw peer (Bay Networks or otherwise) receives a broadcast response from an unconfigured peer on a Bay Networks router, the local peer opens a DLSw connection to the unconfigured peer.

Figure 3-5 shows the sample network of three routers running DLSw. This network uses the following Peer IP Table entries:

- Router A's Peer IP Table has a single entry, as follows:
  - — The DLSw single switch communication with Router B does not require an entry in the Peer IP Table.
  - — The connection to Router C uses dual switch DLSw. An entry is required in the Peer IP Table so that Router A can forward DLSw broadcasts to Router C. The circuitless IP address of Router C (192.32.200.1) is entered into Router A's Peer IP Table, since this value is the only value in Router C's Slot Table.
- Router B communicates to Router A via a single switch connection. No Peer IP Table is required for Router B.
- Router C communicates with Router A using dual switch mode. The circuitless IP address of Router A (192.32.100.1) is entered into Router C's Peer IP Table. However, you can use any IP address in Router A's Slot Table instead of the circuitless IP address.

When using dual switch mode, DLSw is not configured on the links between the routers. Only IP must be configured on these interfaces.When communicating using single switch mode, DLSw is configured on the connecting interfaces.

Note that either link from Router A to Router C can be used to transport DLSw traffic. IP determines which link will be used for these routers to communicate.

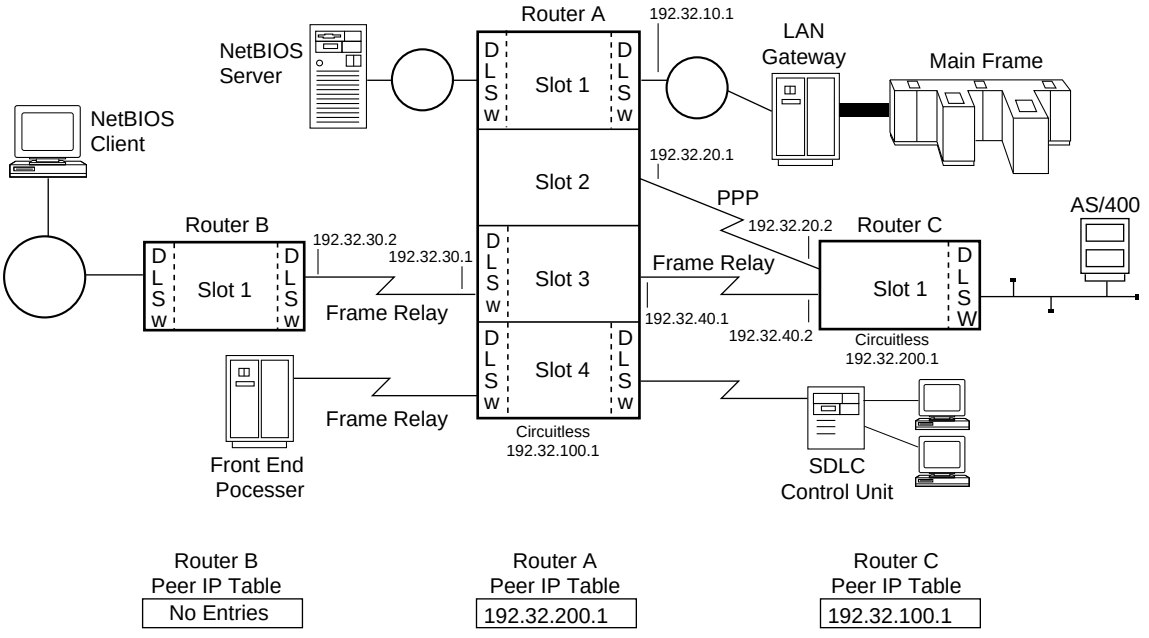


Figure 3-5. Sample Network with Peer IP Table Definitions

Configuration Objects for SDLC

This section describes the objects you define when you configure DLSw SDLC-attached devices on the router, specifically,

- SDLC line parameters
- DLSw Local Devices

SDLC Line Parameters

DLSw uses the SDLC Line Parameters to determine the characteristics of the link. You must set these parameters to allow the router to communicate with the SNA equipment. Following is a brief description of the major parameters:

- Clock Source

  Use this parameter when connecting the SNA equipment directly to the router. Either the router or the SNA equipment can define the speed of the SDLC link. You must configure one device to internal clocking, and the other device to external clocking. The Clock Source parameter identifies whether the router provides clocking (INTERNAL) or receives clocking (EXTERNAL) from the other device.

  When connected to a modem, set this parameter to EXTERNAL. The attached modem provides the clocking for the connection.

Note: *When connecting the router directly to an SNA endstation, the cables connecting these devices must connect the "transmit" pins of one device to the "receive" pins of the other. Typically, a DCE cable for the SNA equipment is connected to a Bay Networks Synchronous Passthrough cable. Conversely, an SNA DTE cable connects to a Bay Networks modem cable.*

- Internal Clock Speed

  Use this parameter to specify the speed of the line. It is relevant only when "Clock Source" is set to INTERNAL.

  Attached devices must be capable of operating at the specified speed. Some of the more common allowed speeds for IBM products are as follows:

  — An IBM 3274 with an V.24/RS-232 interface supports up to 9600 bps. Later models support speeds up to 19200 bps.

  — An IBM 3274 with a V.35 interface supports up to 56 Kb/s.

  — An IBM 3174 with a V.24/RS-232 interface supports up to 19200 bps.

  — An IBM 3174 with a V.35 interface and running Licensed Internal Code-C supports up to 256 Kb/s.

- Sync Line Coding

  Use this parameter to set the same line coding value for all devices attached to the same SDLC link. The network administrator can define the line coding for most SNA control units.

  The Sync Line Coding parameter does not operate with the Bay Networks AFN® and the Quad Sync module.

For information on configuring the SDLC line parameters, refer to Chapter 4.

Local Devices

DLSw uses Local Device entries to define SDLC-attached SNA physical units (PUs) to the router. NetBIOS does not support SDLC-attached devices.

To take advantage of integrated SDLC services in DLSw, you must define the SDLC devices that you want to appear as natively attached to the LAN. When you define such devices, you map the devices to LAN MAC and SAP addresses.

You can add Local Devices at the following times:

- When you add SDLC to a synchronous circuit and add the DLSw protocol to that circuit.
- When you edit a synchronous circuit that already has SDLC and DLSw on it.
- When you edit DLSw interface parameters. In this case, the interface whose parameters you edit must already have at least one local device defined on it. .

Several Local Device parameters must match other entries in the router, or in the attached SDLC device. These include:

- Link Address (hex)

  This parameter must match the polling address defined in the SDLC-attached device.

- PU Type

  This parameter must match the PU type of the SDLC-attached device. For some devices, this is a fixed value. For example, the IBM 3274 is a PU2.0, while the IBM 5494 is a PU 2.1. For other devices, it is explicitly defined. For example, the IBM 3174 can be configured as PU 2.0 or PU 2.1.

- IDBLOCK and IDNUM

  These parameters (required for PU 2.0 devices only) must match the same values on the host. The 3-digit IDBLOCK and the 5-digit IDNUM may be defined on the host as a single 8-digit XID.

- XID Format

  This parameter is typically set to FIXED for PU 2.0 devices, and set to NEGOTIABLE2 for PU 2.1 devices.

- Source (Host) MAC (hex)

  This parameter must be defined in the LAN gateway when using an IBM 3174 (or compatible) gateway. Other gateways typically do not define this value.

- Destination (Host) MAC (hex)

  This parameter must match the MAC address of the LAN gateway, using MSB (Token Ring) format.

- Source (Virtual) SAP (hex) and Destination (Host) SAP (hex)

  These parameters must be entered into the SAP Table of the source and destination routers. Both parameters default to 04. This value is included in the default SAP Table.

For each local device you add, Site Manager creates a corresponding SDLC link station, which is how SDLC sees the local device. Site Manager assigns several default parameter values to the link station. For information on how to access and change the link station parameters, see *Configuring SDLC Services*.

Once you add local devices, you can access and change the local device parameters, as described in Chapter 5.

Optional Configuration Objects

Bay Networks routers in your network learn about the locations of remote NetBIOS and SNA systems that are accessible through DLSw services in two ways:

- Through a dynamic process, where DLSw inspects incoming frames to learn the location of remote endstations.
- Through static definitions where the network administrator defines the location of NetBIOS and SNA systems attached to remote LANs. Static definitions are never required, but may be used to reduce the amount of broadcast messages traversing the network.

Dynamically Learned Remote Systems

Bay Networks routers cache (dynamically learn) the MAC address and NetBIOS name of remote systems.

Local Bay Networks routers receive frames that contain information about the location (that is, the DLSw peer IP address) of each remote system that uses DLSw services. This information is learned from broadcast frames (TESTs, XIDs and NetBIOS) generated by the remote endstations or applications. The router stores this information in separate NetBIOS and MAC caches.

The router uses the learned IP address to locally specify the DLSw peer that can reach the desired endstation. The cache is not used for forwarding traffic during the first LLC2 session, but will be used in new sessions with that endstation.

You can set a timer value that determines when NetBIOS or MAC cache entries in the router disappear. The timer parameters are NetBIOS Cache Age and MAC Cache Age. When the cached entry goes unused for the specified cache age time, or becomes unreachable to new queries, it is removed from the cache and subsequent frames are broadcast to all configured peers.

The router refreshes a cache entry when DLSw services establish a connection to the NetBIOS or SNA system associated with that entry. (The router resets the appropriate Cache Age timer to its maximum wait interval.)

Statically Defined Remote Systems

To reduce DLSw broadcasts, you can define the IP addresses of DLSw peers that can reach remote systems or applications associated with specific NetBIOS names or MAC addresses. This information augments any information that the router's MAC and NetBIOS caching mechanisms learn dynamically.

Static entries can exist in two tables:

- Default MAC Peer IP Table

  Each entry in this table contains a MAC address and the IP address of a DLSw peer which can forward packets to this MAC address.

- Default NetBIOS Peer IP Table

  Each entry in this table contains the NetBIOS name and the IP address of the DLSw peer to which this NetBIOS device is connected.

In the local router's Default NetBIOS Peer IP Table, enter the IP address of the remote peer associated with any remote NetBIOS application you need to reach through DLSw services. Each entry in this table associates the name of a NetBIOS client with the IP address of the DLSw peer that can reach that client.

In the router's Default MAC Peer IP Table, enter the peer IP address of the DLSw peer associated with any remote SNA system or application that you need to reach through DLSw services. Each entry in this table associates the MAC address for an SNA system with the IP address of the DLSw peer that can reach that system.

Unlike dynamically learned entries, statically defined entries remain unless you delete them from the Default NetBIOS Peer IP Table or the Default MAC Peer IP Table.

See Chapter 5 for more information on editing the Default NetBIOS Peer IP Table and the Default MAC Peer IP Table.

Chapter 4
Enabling DLSw Services

This chapter describes how to enable DLSw services. It assumes you have read *Configuring Routers* and completed the following steps:

1. Opened a configuration file
2. Specified router hardware if this is a local-mode configuration file
3. Selected the link- or net-module connector on which you are enabling DLSw

When you enable DLSw, you are required to specify some of the parameters; the Configuration Manager supplies default values for the others. If you want to edit the other parameters, see Chapter 5, “Editing DLSw Parameters.”

Appendix A provides a quick reference to the default DLSw parameter settings. You may want to review these settings before editing your DLSw configuration.

Enabling DLSw on an Interface

To enable DLSw on an interface, start at the Select Protocols window and select DLSw. The Select Protocols window appears after you select a link- or net-module connector to which you are configuring DLSw.

The steps you take to enable DLSw services depend on whether you are enabling it:

- For the first time or a subsequent time
- On Token Ring/802.5 or other SRB networks, or on Ethernet/802.3 or Frame Relay

Configuring DLSw the First Time

When you first configure DLSw, you use Site Manager windows to

- Set the DLSw global parameters
- Add Source Routing global parameters (Token Ring or other, or if you choose to use SRB encapsulation on Ethernet or Frame Relay)
- Enter Frame Relay mapping information (Frame Relay without SRB encapsulation)
- Set slot IP addresses
- Add peer IP addresses
- Add service access points (SAPs)
- Edit SDLC line parameters and SDLC local devices

Setting the DLSw Global Parameters

After you select DLSw from the Select Protocols window, the DLSw Global Parameters window appears (Figure 4-1). To set the DLSw global parameters, follow these steps.

1. **Edit the IP Virtual Ring parameter.**
2. **Click on OK.**

This enables the DLSw global parameters.

Figure 4-1. DLSw Global Parameters Window

Parameter:	**IP Virtual Ring**
Default:	None
Range:	1 to 4095
Function:	Specifies a virtual ring number for the TCP/IP network cloud.
Instructions:	Enter any valid ring number. The number should match the ring number chosen by other DLSw peers on the same network cloud. Make sure that the number is unique among any other Ring IDs, Group LAN IDs, or Internal LAN IDs assigned in the network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.5

Note: *The IP Virtual Ring and Virtual Ring MTU parameters that appear in the DLSw Global Parameters window are primarily for compatibility with SRB networks locally attached to the router. However, Site Manager requires you to enter a value for the IP Virtual Ring, even if you are configuring DLSw services on non-SRB segments locally attached to the same router.*

Specifying Source Routing Bridge Encapsulation

The Source Route Encapsulation dialogue box (Figure 4-2) allows you to specify the type of encapsulation formats to be used on Ethernet/802.3 and Frame Relay interfaces running DLSw. Click on Cancel if you are configuring standard LLC2 over Ethernet, or if you are configuring Frame Relay using the RFC 1490 Routing Standard. Click on OK if you want to configure Bay Networks proprietary SRB over Ethernet or Frame Relay using the RFC 1490 Bridging Standard.

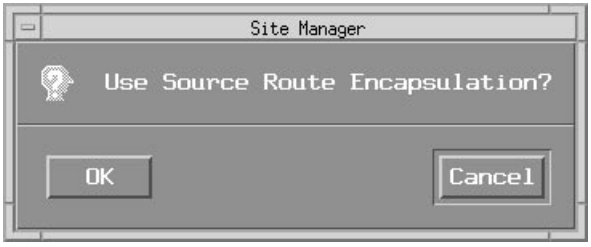


Figure 4-2. Source Route Encapsulation Dialogue Box

Adding Source Routing Parameters

When you add DLSw to a Token Ring circuit, you first set the source routing global parameters. If you have not yet enabled source routing on any circuit, the first window to appear is the Source Routing Global Parameters window. If you have enabled source routing on some other circuit, the first window to appear is the Source Routing Interface Parameters window.

See *Configuring Bridging Services* for detailed information on configuring the necessary source routing parameters.

The Ethernet configuration does not require the source routing steps.

Mapping Frame Relay Addresses

If you are configuring a Frame Relay circuit without SRB, the LLC2 Frame Relay Mappings window appears (Figure 4-3).

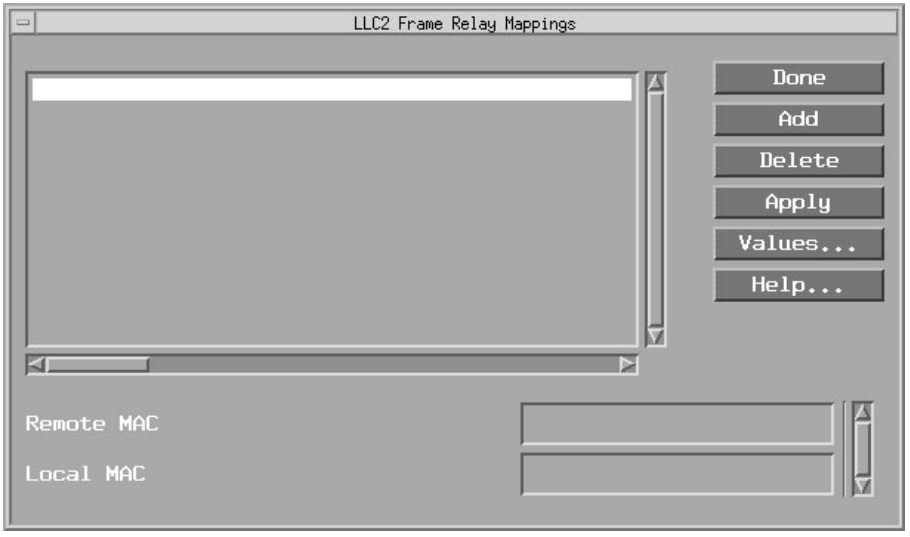


Figure 4-3. LLC2 Frame Relay Mappings Window

1. **Select Add.**

   The LLC2 Frame Relay Mapping Add window appears (Figure 4-4).

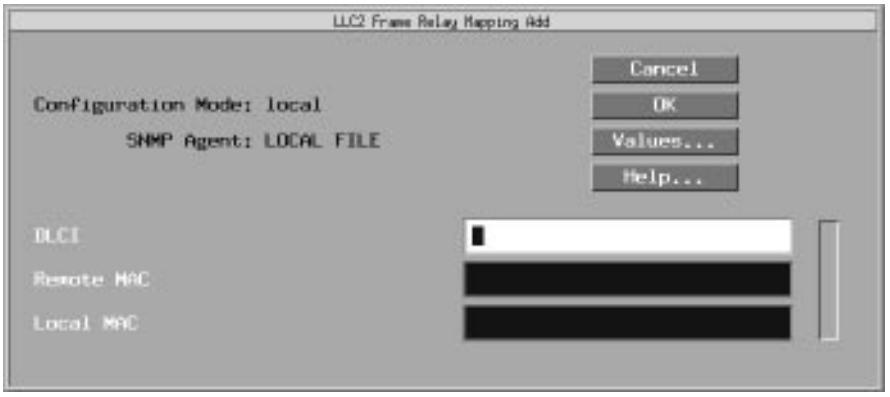


Figure 4-4. LLC2 Frame Relay Mapping Add Window

2. **Specify the DLCI, Remote MAC, and Local MAC parameters, as follows.**
3. **Click on OK.**

   The Configuration Manager returns to the LLC2 Frame Relay Mappings window, which now lists the selected circuit.

For more information on mapping DLCIs to MAC addresses, refer to *Configuring LLC Services*.

Parameter:	**DLCI**
Default:	None
Options:	Standard Data Link Connection Identifier (DLCI) numbers in hexadecimal format
Function:	Provides the number of the virtual circuit to which the local or remote MAC address will be mapped.
Instructions:	Enter a hexadecimal DLCI number assigned by your system administrator or Frame Relay provider.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.6.9.1.3

Parameter:	**Remote MAC**
Default:	None
Options:	Standard MSB Token Ring MAC addresses
Function:	Provides the remote MAC address, mapping outgoing requests for this MAC address corresponding to the DLCI value. The Remote MAC address must be unique, with only DLCI mapping for the specific MAC address.
Instructions:	Enter the remote MAC address of the host. If you need to specify the real hardware address of the host, enter it as an octal string.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.6.9.1.5

Parameter:	**Local MAC**
Default:	None
Options:	Standard MSB Token Ring MAC addresses
Function:	Provides the local MAC address, mapping incoming requests on this DLCI to that address. The Local MAC address must be unique, with only DLCI mapping for the specific MAC address.
Instructions:	Enter the MAC address of the recipient.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.6.9.1.4

Adding Slot IP Addresses

The DLSw Slot Configuration window (Figure 4-5) displays a list of the slot IP addresses you have added.

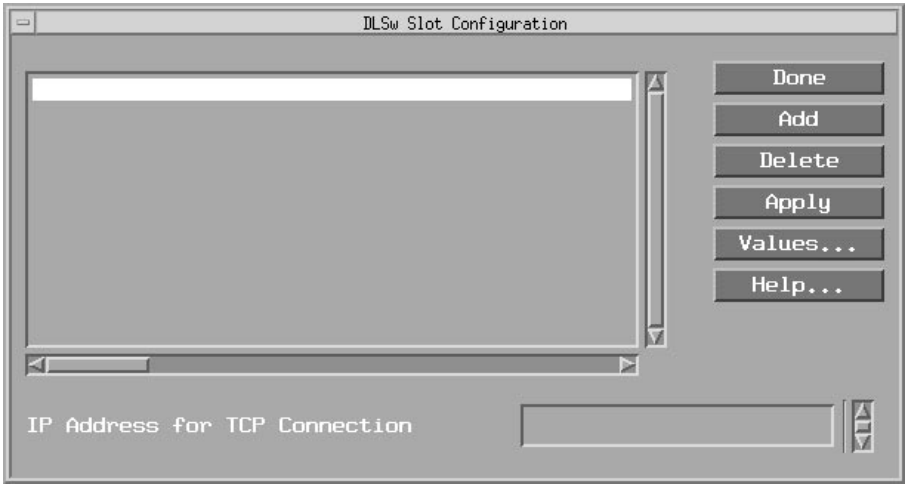


Figure 4-5. DLSw Slot Configuration Window

1. **Click on Add.**

   The second DLSw Slot Configuration window appears (Figure 4-6).

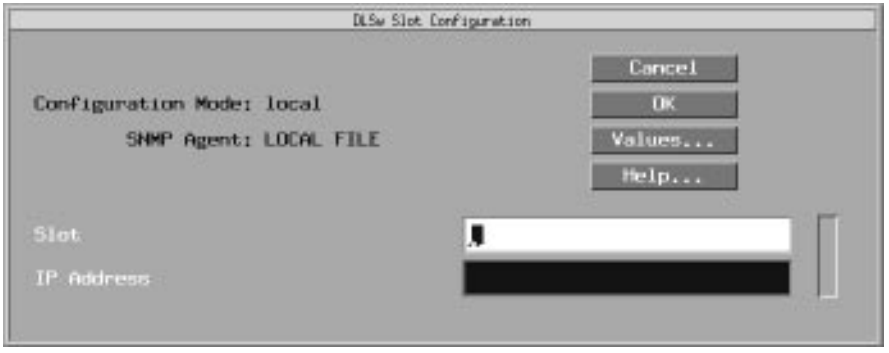


Figure 4-6. Add DLSw Slot Configuration Window

2. **Enter the appropriate slot value and its IP address.**

   Use the following parameter descriptions as a guide.

3. **Click on OK.**

   The DLSw Slot Configuration window reappears. Repeat the instructions in this section for each slot you want to add.

4. **Click on Done.**

Parameter:	**Slot**
Default:	None
Range:	1 to 14
Function:	Specifies the slot number associated with the Token Ring or Ethernet interface over which DLSw is running.
Instructions:	Enter a slot number that is valid for running DLSw, considering the router model and the slots that link modules can occupy. You should enter only slots running DLSw.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.3.1.2

Parameter:	**IP Address**
Default:	None
Options:	Any IP address specified in dotted decimal notation
Function:	Specifies a unique IP address for each slot running DLSw on the router. The address cannot be reused on another slot. The IP address specifies where the TCP connection for DLSw terminates.
Instructions:	Enter the appropriate IP address. If a circuitless IP address is configured, use that address for this parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.3.1.3

Adding DLSw Peer IP Addresses

The DLSw Peer Configuration window (Figure 4-7) displays a list of the peer IP addresses you have added.

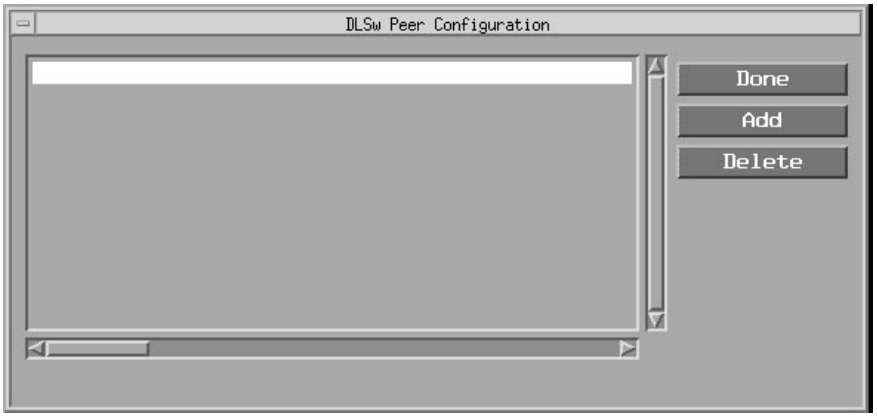


Figure 4-7. DLSw Peer Configuration Window

1. **Click on Add.**

   The second DLSw Peer Configuration window appears (Figure 4-8).

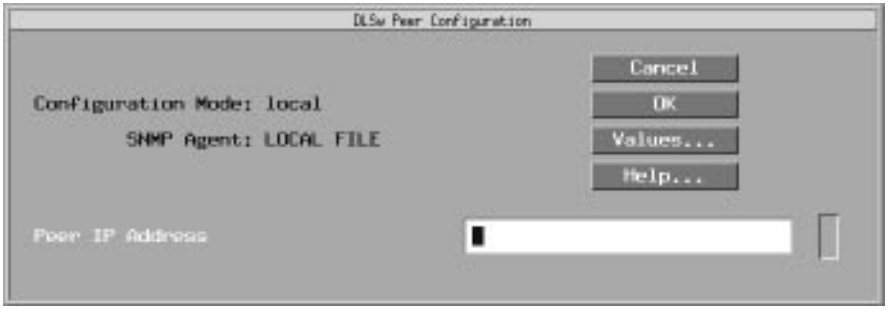


Figure 4-8. Add DLSw Peer Configuration Window

2. **Enter the appropriate peer IP address.**

   Use the following parameter description as a guide.

3. **Click on OK.**

This accepts the peer IP address and displays the first DLSw Peer Configuration window. Add additional peers by clicking on Add and repeating the procedure as many times as needed.

4. **Click on Done.**

Parameter:	**Peer IP Address**
Default:	None
Options:	Any valid, 32-bit IP address of the form: *network.host* (using dotted decimal notation)
Function:	Specifies the IP address of a remote DLSw peer. Once added to the DLSw peer table, this address defines a “configured peer” on the local router. Configured peers receive all DLSw-related broadcast frames for a given router or network processor.
Instructions:	Enter the IP address at which the configured peer will receive all DLSw-related broadcast frames.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.5.1.3

Adding a Service Access Point (SAP)

The DLSw SAP Configuration window (Figure 4-9) displays SAP configuration information and lists the predefined SAP addresses.

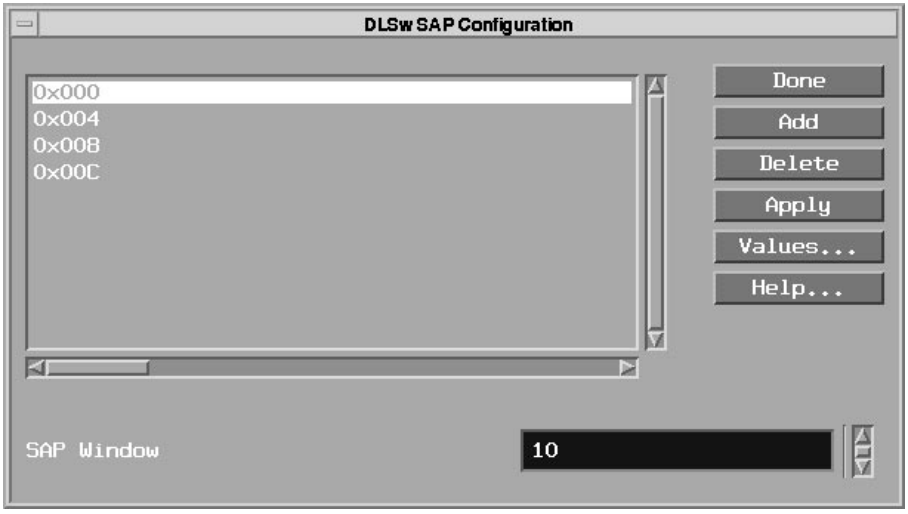


Figure 4-9. DLSw SAP Configuration Window

1. **Click on Add.**

   The second DLSw SAP Configuration window appears (Figure 4-10).

Figure 4-10. Add DLSw SAP Configuration Window

2. **Enter the appropriate SAP value.**

   Refer to the parameter description that follows as a guide.

3. **Click on OK.**

The first DLSw SAP Configuration window reappears. Repeat the instructions in this section as needed.

4. **Click on Done.**

   The main Configuration Manager window appears. You have now completed your initial installation of DLSw. If you have not already configured the IP addresses of the slots and connection to the IP network, add them now.

Parameter:	**SAP**
Default:	None
Options:	An even-numbered SAP address (00, 04 to EC, F0) in hexadecimal format
Function:	Specifies the destination service access point address (SAP) associated with a communication subsystem on a remote device (for example, on a PC or host).
Instructions:	Begin the address with *0x* and specify the SAP address associated with a specific communication subsystem. The SAP entries for SNA are 0x04, 0x08, and 0x0C. The SAP entry for NetBIOS is 0xF0.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.4.1.2

Editing SDLC Line Parameters and SDLC Local Devices

To configure DLSw on synchronous interfaces (COM1, COM2, etc.) using the SDLC protocol:

1. **Select SDLC from the WAN protocols window.**

   The Configuration Manager displays the SDLC Line Parameters window (Figure 4-11).

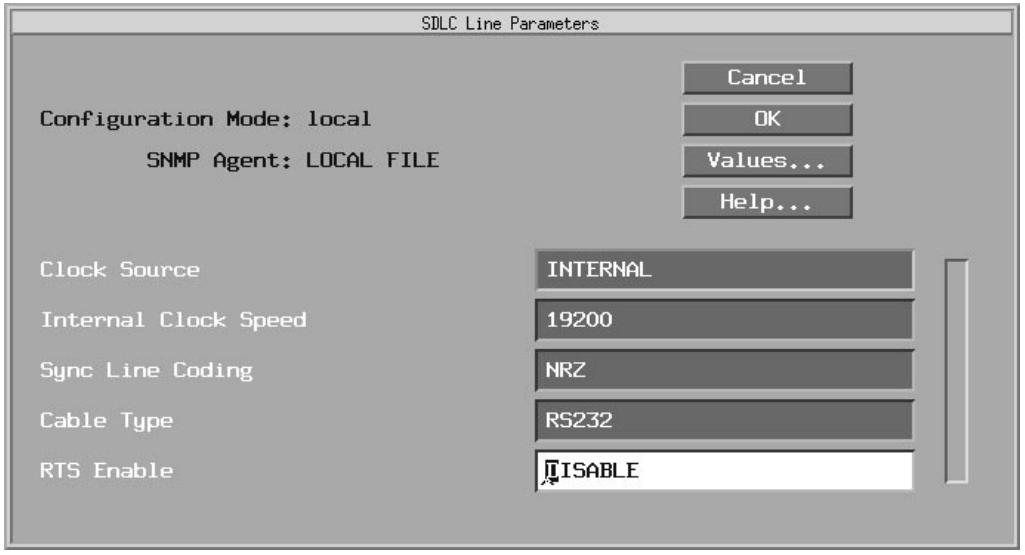


Figure 4-11. SDLC Line Parameters Window

2. **Edit the Clock Source, Internal Clock Speed, Sync Line Coding, Cable Type, and RTS Enable parameters, as follows:**

Parameter:	**Clock Source**
Default:	Internal
Options:	External | Internal
Function:	Specifies the origin of the synchronous timing signals. If you set this parameter to Internal, this router supplies the required timing signals. If you set this parameter to External, an external network device supplies the required timing signals.
Instructions:	Set this parameter to either Internal or External, as appropriate for your network.
MIB Object ID:	1.3.6.1.4.1.18.3.4.5.1.13

Parameter:	**Internal Clock Speed**
Default:	64 KB
Options:	1200 B| 2400 B | 4800 B | 7200 B | 9600 B | 19200 B | 32000 B | 38400 B | 56 KB | 64 KB | 125 KB | 230 KB| 420 KB | 625 KB | 833 KB | 1.25 MB | 2.5 MB | 5 MB
Function:	Sets the clock speed of an internally supplied clock when Clock Source is set to Internal.
Instructions:	Click on Values and set the clock speed for the internal clock to the desired data transmission rate across the synchronous line. This parameter is unavailable when Clock Source is set to External.
MIB Object ID:	1.3.6.1.4.1.18.3.4.5.1.14

Parameter:	**Sync Line Coding**
Default:	NRZ
Options:	NRZ | NRZI | NRZI Mark
Function:	This parameter specifies the line coding of the physical synchronous line. You can change the value of this parameter to match the line coding of a device at the other end of the line. This parameter is relevant only for the AN and the ASN routers. Other Bay Networks router platforms use NRZ encoding. *NRZ* — Indicates Non-Return to Zero encoding. *NRZI* — Indicates Non-Return to Zero Inverted encoding. *NRZI Mark* — Indicates Non-Return to Zero Inverted Mark encoding.
Instructions:	Select the appropriate value for synchronous line coding.
MIB Object ID:	1.3.6.1.4.1.18.3.4.5.1.88

Parameter:	**Cable Type**
Default:	Null
Options:	Null | RS232 | RS422 | V35 | X21
Function:	Specifies the cable interface to the network.
Instructions:	Select the cable interface that you are using to connect to the network.
MIB Object ID:	1.3.6.1.4.1.18.3.4.5.1.83

Parameter:	**RTS Enable**
Default:	Disabled
Options:	Enabled | Disabled
Function:	Controls the toggling of the Request to Send (RTS) signal on the interface. For manual dial modems (2-wire), you should set this parameter to Enabled. For leased modems (4-wire), the setting should be Disabled.
Instructions:	Click on Values and select Enabled or Disabled.
MIB Object ID:	1.3.6.1.4.1.18.3.4.5.1.16

3. **Click on OK.**

   The Select Protocols window appears (Figure 4-12).

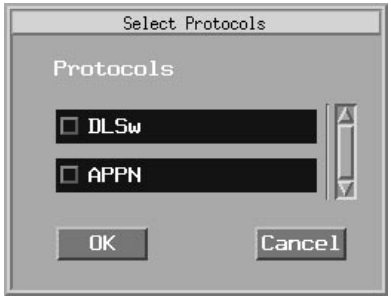


Figure 4-12. Select Protocols Window

4. **Select DLSw and click on OK.**

The DLS Local Device Configuration window appears (Figure 4-13).

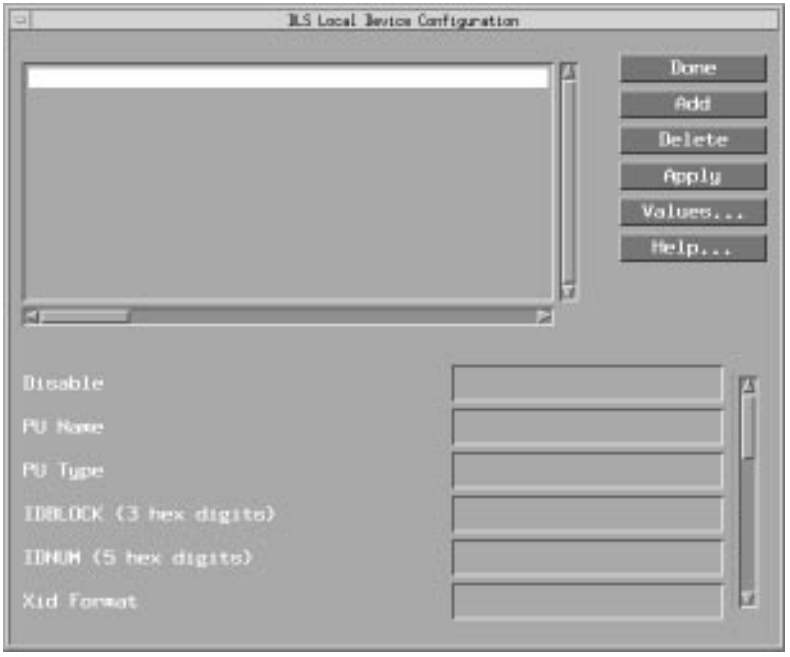


Figure 4-13. DLS Local Device Configuration Window

5. Click on Add.

The Local Device Configuration screen appears (Figure 4-14). To take advantage of integrated SDLC services in DLSw, you must define the SDLC devices that you want to appear as natively attached to the LAN. When you define such devices, you map the devices to LAN MAC and SAP addresses.

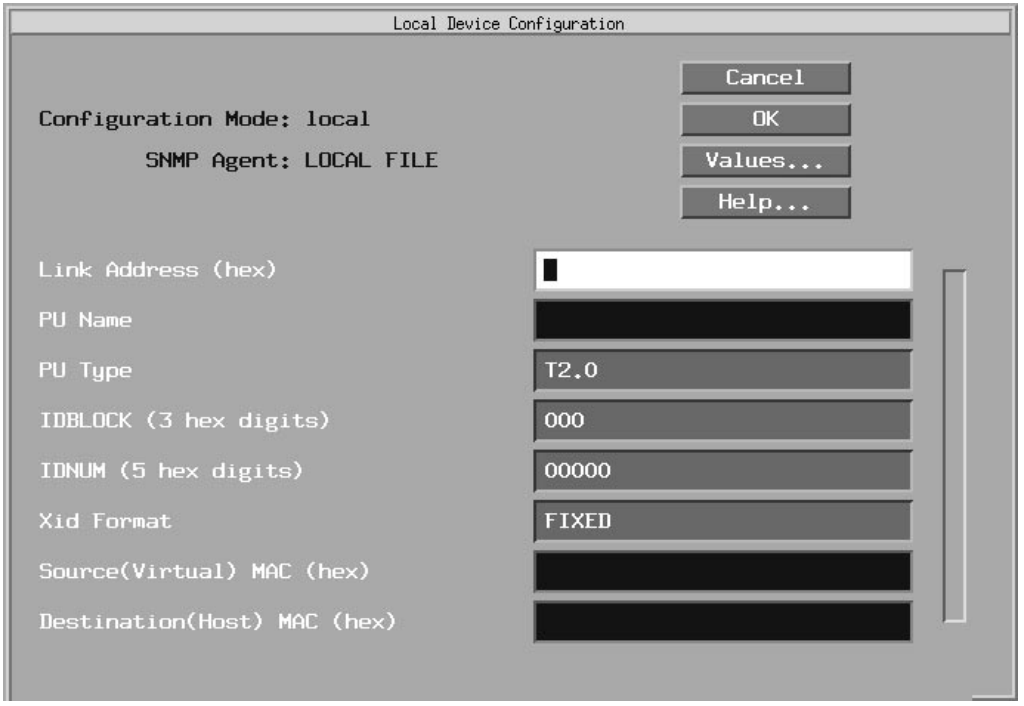


Figure 4-14. Local Device Configuration Window

Parameter:	**Link Address (hex)**
Default:	None
Range:	Any valid hexadecimal link station address from 0x01 to 0xFE
Function:	Specifies the address of the link station.
Instructions:	Type 0x followed by the link station address.
MIB Object ID:	N/A

Parameter:	**Disable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables the DLSw local device.
Instructions:	Set to Disable if you want to temporarily disable the local device, rather than delete it. Set to Enable if you want to reinitialize the local device.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.2

Parameter:	**PU Name**
Default:	None
Options:	Any valid, 8-byte ASCII name
Function:	Specifies the name of the adjacent link station. This name uniquely identifies the station for statistics and Alert messages.
Instructions:	Enter the 8-byte ASCII link station name.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.7.5.1.32

Parameter:	**PU Type**
Default:	None
Options:	T2.0 | T2.1
Function:	Specifies the type of the XID-sending node. This parameter is used with the IDBLOCK, IDNUM, and XID Format parameters to determine the station exchange identification (XID) value.
Instructions:	Choose either T2.0 or T2.1.
MIB Object ID:	N/A

Parameter:	**IDBLOCK**
Default:	None
Options:	017 | 061 | any other 3-digit hexadecimal value
Function:	Specifies the block number, which must match the host's IDBLOCK parameter value that identifies incoming connection requests. This parameter is used with the PU Type, IDNUM, and XID Format parameters to determine the station exchange identification (XID) value.
Instructions:	Obtain the configured value at the host (from VTAM or other host operating system) for this device. In most cases: — Enter 017 for a 3174 in T2.0 mode. — Enter 061 for a T2.0 node in fixed format.
MIB Object ID:	N/A

Parameter:	**IDNUM**
Default:	None
Options:	Any 5-digit hexadecimal value from 00000 to FFFFF (for T2.0 nodes)
Function:	Specifies the ID number, which must match the host's IDNUM parameter value that identifies incoming connection requests. This parameter is used with the PU Type, IDBLOCK, and XID Format parameters to determine the station exchange identification (XID) value.
Instructions:	Obtain the configured value at the host (from VTAM or other host operating system) for this device. Enter a 5-digit hexadecimal value from 00000 to FFFFF for T2.0 nodes.
MIB Object ID:	N/A

Parameter:	**XID Format**
Default:	None
Options:	FIXED | VARIABLE1 | VARIABLE2
Function:	Specifies the format of the XID I-field.
Instructions:	Enter one of the following options: FIXED Fixed format (for T2.0) VARIABLE1 Variable format (for T1/T2.0/T2.1 to T4/T5 node exchanges) VARIABLE2 Variable format (for T2.1 to T2.1/T4/T5 node exchanges)
MIB Object ID:	N/A

Parameter:	**Source (Virtual) MAC (hex)**
Default:	None
Options:	Any standard MSB Token Ring MAC address
Function:	Specifies the source MAC address of an emulated Token Ring endstation for this device.
Instructions:	Enter the 12-digit hexadecimal source MAC address you want to assign to the SDLC device. The address should be in MSB format, and it should be unique in the network (even among other source addresses on the router).
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.6

Parameter:	**Source (Virtual) SAP (hex)**
Default:	0x4
Range:	0x01 to 0xFE
Function:	Specifies the source service access point (SAP) of an emulated Token Ring or Ethernet endstation for this device.
Instructions:	Begin the address with 0x and enter a 1-digit or 2-digit hexadecimal source SAP address associated with this device. Typical values are multiples of 4.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.7

Parameter:	**Destination (Host) MAC (hex)**
Default:	None
Options:	Any standard MSB Token Ring MAC address
Function:	Identifies (with the Destination SAP) the Token Ring or Ethernet host the local device will reach via SDLC services.
Instructions:	Consult your host system manager for the host MAC address; then enter the 12-digit hexadecimal address.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.8

Parameter:	**Destination (Host) SAP (hex)**
Default:	0x4
Range:	0x01 to 0xFE
Function:	Identifies (with the Destination MAC) the Token Ring or Ethernet host the local device will reach via SDLC services.
Instructions:	Consult your host system manager for the host SAP address. Enter the 0x prefix followed by a 1-digit or 2-digit hexadecimal address.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.9

Parameter:	**MAXOUT**
Default:	7
Range:	1 to 127
Function:	Controls the maximum number of consecutive frames that an SDLC link station can send without acknowledgment.
Instructions:	Enter a value from 1 to 127.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.7.5.1.10

Parameter:	**MAXDATA**
Default:	2057
Options:	265 | 521 | 1033 | 2057
Function:	Specifies the maximum frame size SDLC supports. This value includes the Transmission Header (TH) and Request Header (RH).
Instructions:	Enter a maximum frame size equal to or larger than the largest frame size that will be received.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.7.5.1.7

Parameter:	**Canureach Timer**
Default:	30 seconds (s)
Range:	0 to 3600
Function:	Specifies the time interval (in seconds) after which the router sends a *canureach* message to the remote DLSw peer to establish a session.
Instructions:	Enter the number of seconds you want for the time interval. For example, enter 1 to transmit a *canureach* message once per second, or enter 3600 to transmit the message once per hour. Enter 0 if you do not want to transmit a *canureach* message.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.11

Parameter:	**Canureach Retries**
Default:	4294967295
Range:	0 to 4294967295
Function:	Specifies the number of times a *canureach* message is sent to the remote DLSw peer to establish a session.
Instructions:	Enter the number of retries you want. Enter 0 if you do not want to transmit *canureach* messages. Leave the default value 4294967295 to send an infinite number of *canureach* messages for this connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.12

Parameter:	**Link Station Timer**
Default:	30 seconds
Range:	0 to 3600
Function:	Sets the time interval (in seconds) after which the router sends a connect request to the local SDLC device to establish a session.
Instructions:	Enter the number of seconds you want for the time interval. For example, enter 1 to send a connect request once a second, or enter 3600 to send a connect request once an hour. Enter 0 if you do not want to send connect requests.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.13

Parameter:	**Link Station Retries**
Default:	4294967295
Range:	0 to 4294967295
Function:	Specifies the maximum number of times that a connect request is sent to the local SDLC device to establish a session.
Instructions:	Enter the number of retries you want. Enter 0 if you do not want to send connect requests. Leave the default value 4294967295 to send an infinite number of connect requests for this connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.14

Parameter:	**SDLC Receive Credit**
Default:	10
Range:	0 to 200
Function:	Specifies the maximum number of frames SDLC can send to DLSw. This is a flow control parameter.
Instructions:	Enter the maximum number of frames you want SDLC to send to DLSw. For example, enter 1 if you want DLSw to accept 1 frame from SDLC before it updates the SDLC credit. Enter 0 if you want DLSw to receive an infinite number of frames from SDLC without updating the SDLC credit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.15

Parameter:	**SDLC Transmit Credit**
Default:	10
Range:	0 to 200
Function:	Specifies the maximum number of frames DLSw can send to SDLC.
Instructions:	Enter the maximum number of frames you want DLSw to send to SDLC. For example, enter 1 if you want DLSw to send only one frame to SDLC until it receives a credit update from SDLC. Enter 0 if you want DLSw to send an infinite number of frames to SDLC without updating the SDLC credit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.16

Subsequent DLSw Configuration

If you have an existing DLSw configuration on your router, configuring DLSw on other interfaces is simpler.

When you select DLSw on an Ethernet circuit, no further steps are needed.

When you select DLSw on a Token Ring circuit, the Source Routing Edit Interface window appears. See *Configuring Bridging Services* for detailed information on this window. When you are finished, click on OK.

The main Configuration Manager window appears. You have now completed the installation of DLSw. If you have not already configured the IP addresses of the slots and connection to the IP network, add them now.

Chapter 5
Editing DLSw Parameters

This chapter describes how to edit DLSw global and interface parameters, as well as how to add, edit, and delete the following configuration objects:

- Configured peers
- Slots
- Service access points (SAPs)
- Default NetBIOS peers
- Default MAC peers
- Local devices

This chapter also describes how to delete DLSw services from all circuits simultaneously.

The Site Manager sequence for adding the first DLSw interface to your router configuration first requires you to define an initial set of DLSw configured peers, slots, and SAPs.

Using the Parameter Descriptions

Each DLSw parameter description provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, see *Using Technician Interface Software*.

Caution: *The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.*

You may want to customize the LLC2, TCP/IP, APPN, SDLC, or source routing bridge parameters as well, since these support DLSw services on the router. If so, refer to one of the guides listed in Table 5-1. Otherwise, you can access parameters of the DLSw support protocols from the Protocols menu of the Configuration Manager window or the Circuit Definition window.

Table 5-1. Customizing the DLSw Support Protocols

Protocol	Refer To
TCP	*Configuring TCP Services*
IP and IP RIP	*Configuring IP Services*
Source routing bridge	*Configuring Bridging Services*
LLC2	*Configuring LLC Services*
SDLC	*Configuring SDLC Services*
APPN (DLSw local circuit definition)	*Configuring APPN Services*

Accessing DLSw Parameters

To access and edit DLSw parameters, begin at the Configuration Manager window and select Protocols→DLSw (Figure 5-1).

Figure 5-1. Configuration Manager Window

Editing DLSw Global Parameters

To edit DLSw global parameters, begin at the Configuration Manager window (Figure 5-1) and then

1. **Select Protocols→DLSw→Global.**

   The Edit DLSw Global Parameters window appears (Figure 5-2).

Figure 5-2. Edit DLSw Global Parameters Window

2. **Edit the parameters you want to change.**
3. **Click on OK.**

   This saves your changes and returns you to the Configuration Manager window.

DLSw Global Parameter Descriptions

This section describes the DLSw global parameters that you can customize from the Edit DLSw Global Parameters window.

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Globally enables or disables the system software mechanisms that allow you to add DLSw interfaces to the node configuration. *Disable* — Switches every DLSw interface enabled on the router to the disabled (inactive) state. *Enable* — Reinitializes every DLSw interface on the router, based on • The current setting of the associated Enable parameter • The current state of the associated circuit
Instructions:	Select Disable to switch every DLSw interface existing on the node to the inactive state. Select Enable to globally reinitialize all DLSw interfaces configured on the node.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.2

Parameter:	**TCP Window Size**
Default:	8000 (octets)
Range:	5000 to 64000 (octets)
Function:	Specifies (in octets) the maximum amount of DLSw data that the local and remote TCP entities can send before requiring an acknowledgment, or can receive before acknowledging.
Instructions:	Type in any valid number of octets. If the TCP Window Size value for DLSw services is less than the global TCP Max Window value, DLSw uses its own TCP Window Size. If the TCP Window Size for DLSw services is greater than the global TCP Max Window size, Site Manager prompts you to make one of the following choices: • Increase the global TCP Max Window size to the TCP Window Size set for DLSw services. • Accept the global TCP Max Window size as the TCP Window Size for DLSw services on the router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.4

Note: *The default value is based on both NetBIOS and SNA traffic. NetBIOS can have frame size up to 4 KB, but the default virtual ring MTU limits the frame size on the TCP/IP network to 2 KB (unless changed). SNA uses small frames so this window size can be smaller with SNA-only environments than in environments which include NetBIOS traffic. Keep the window as small as possible. This allows the best (most consistent) response time when packets are not excessively queued in TCP. Selection of this parameter depends on the WAN speed and frame size distribution.*

Parameter:	**IP Virtual Ring**
Default:	None
Options:	Any valid, unassigned ring number from 1 to 4095^{10} (0x0001 to 0x0FFF)
Function:	Specifies a virtual ring number for the TCP/IP network.
Instructions:	Type any valid ring number. The number must be • Unique among any other ring IDs, group LAN IDs, or internal LAN IDs assigned in the network • The same as the virtual ring number used by all other DLSw peers on the same TCP/IP network Entering a value for this mandatory parameter prepares the router for DLSw services on Token Ring/802.5 circuits. (Enter a value even if you are presently configuring DLSw services on Ethernet/802.3 circuits only.)
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.5

Note: *The IP Virtual Ring and Virtual Ring MTU parameters that appear in the DLSw Global Parameters window are primarily for compatibility with SRB networks locally attached to the router. However, Site Manager requires you to enter a value for the IP Virtual Ring, even if you are configuring DLSw services on non-SRB segments locally attached to the same router.*

Parameter: **Max Slot Sessions**

Default: 200 (sessions per slot)

Range: 1 to 10000

Function: Specifies the maximum number of LLC2 sessions that a given slot in the router can support for DLSw requirements. Specifying more sessions per slot has the effect of dedicating more memory and processing resources to DLSw interfaces running on the router.

Instructions: If possible, estimate the maximum number of LLC2 sessions that each DLSw peer slot may need to support concurrently. Type a number that

- Meets session support requirements for DLSw services provided on any slot of the router
- Allows a balance between the number of sessions supported for DLSw services on a slot and the amount of resources remaining for other protocols configured on the same slot

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.8

Parameter: **Virtual Ring MTU**

Default: 1500 (bytes)

Options: Any number of bytes equal to or greater than 1

Function: Specifies a Maximum Transmission Unit (MTU) size for frames sent from local, LAN-attached systems to systems on remote LANs. The smallest MTU size supported among all remote LANs in your configuration determines the maximum value of the Virtual Ring MTU parameter for the local router.

Instructions: Type in any number of bytes equal to or greater than 1.

Entering a new value or accepting the default value for this mandatory parameter helps to prepare endstations for the MTUs of remote LANs.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.10

Note: *Ethernet networks support a Maximum Transmission Unit (MTU) size of 1500 bytes, while Token Ring networks support much larger MTUs. When configuring DLSw for local Token Ring-to-Ethernet translation bridge topologies, the Virtual Ring MTU parameter should not exceed 1500. This sets the Token Ring MTU size so that Ethernet endstations can accept the Token Ring traffic.*

Note: *The IP Virtual Ring and Virtual Ring MTU parameters that appear in the DLSw Global Parameters window are primarily for compatibility with SRB networks locally attached to the router. However, Site Manager requires you to enter a value for the IP Virtual Ring, even if you are configuring DLSw services on non-SRB segments locally attached to the same router.*

Parameter:	**MAC Cache Age**
Default:	300 (s)
Options:	Any number of seconds greater than 20
Function:	Specifies the maximum number of seconds that inactive MAC addresses can exist in the MAC-to-DLSw Peer (mapping) cache.
Instructions:	Enter an interval to limit the amount of memory that inactive MAC cache entries consume for DLSw services on the router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.11

Parameter:	**NetBIOS Cache Age**
Default:	300 (s)
Options:	Any number of seconds greater than 20
Function:	Specifies the maximum number of seconds that inactive NetBIOS names can exist in the NetBIOS-to-DLSw Peer (mapping) cache.
Instructions:	Enter an interval to limit the amount of memory that inactive NetBIOS cache entries consume for DLSw services on the router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.12

Parameter:	**Reject Unconfigured Peers**
Default:	Accept
Options:	Accept | Reject
Function:	Specifies whether DLSw peers in this router should allow (Accept) or disallow (Reject) TCP sessions with other DLSw peers not defined in the DLSw Peer Table.
Instructions:	Select Accept if you want to allow TCP sessions with Bay Networks or other DLSw peers not defined in the Peer Table. Select Reject if you want to disallow TCP sessions with Bay Networks or other DLSw peers not defined in the Peer Table. Disallowing TCP sessions prevents the router from learning the IP addresses of other peers in the network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.13

Parameter:	**Keepalive Time (sec)**
Default:	60 (s)
Range:	0 to 2147483647
Function:	Specifies the time interval after which the router sends a DLSw keepalive message to inactive, established TCP connections to verify that the connection is still available. The keepalive time initiates standard TCP operation. TCP operation determines the status of the TCP connection by receiving acknowledgments for transmitted data. If TCP does not receive an acknowledgment for this data after a series of retransmission attempts, it assumes that either a link or remote router is down. TCP then reports this condition to DLSw. This process can take approximately 20 minutes with default configurations. To decrease the notification time for a lost link or a remote router, decrease the TCP Max Retransmission Timeout parameter value. (Refer to *Configuring TCP Services* for information on the Max Retransmission Timeout parameter.) We recommend that the keepalive time interval setting be 30 seconds or greater. Since only one packet is sufficient to initiate the TCP retransmission procedure, short intervals will use additional memory and resources unnecessarily.
Instructions:	Type in the number of seconds you want for the keepalive time interval, or type a 0 to disable the keepalive feature.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.16

Parameter:	**Maximum Package Size**
Default:	1532 bytes
Range:	0 to 2147483647
Function:	Specifies the maximum package size (in bytes) when sending multiple DLSw frames in a single TCP frame for transmission over a wide area network.
Instructions:	Specify a value smaller than the TCP Window Size parameter and less than or equal to the Virtual Ring MTU size for the network minus the size of the TCP/IP and MAC headers.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.23

Parameter:	**Packaging Timeout**
Default:	10 milliseconds (ms)
Range:	0 to 2147483647
Function:	Specifies the time interval (in milliseconds) to delay a package before sending it to TCP. This value is based on the Packaging Threshold parameter. The value should not be greater than the time it takes to send the number of outstanding bytes before packaging begins.
Instructions:	Type any positive integer in the range 0 to 2147483647. Values are in milliseconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.24

Parameter:	**Packaging Threshold**
Default:	20 percent of the TCP window size
Range:	0 to 100 percent (0 indicates no delay)
Function:	Specifies the percentage of the DLSw TCP window that must be in use if DLSw is to delay sending a package (one that is currently being built).
Instructions:	Type a value in the range 0 to 100 percent. A value of 20 percent indicates that if 20 percent of the TCP window size is being used, DLSw issues the delay, as specified by the Packaging Timeout parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.25

Enabling a DLSw Interface

You can use the Configuration Manager to enable or disable a DLSw interface on a specific circuit. To access the DLSw interface parameters from the Configuration Manager window (refer to Figure 5-1).

1. **Select Protocols→DLSw→Interfaces.**

   The DLSw Interface Configuration window appears (Figure 5-3).

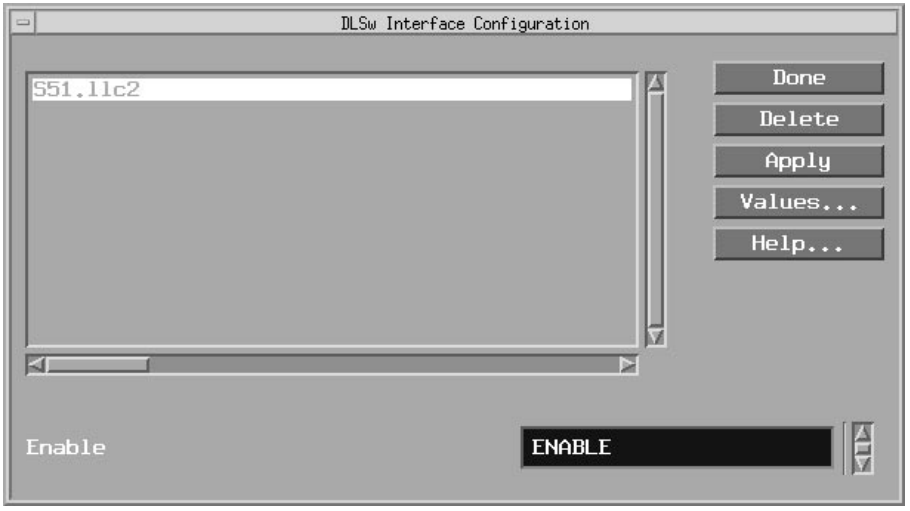


Figure 5-3. DLSw Interface Configuration Window

2. **Select an interface from the list.**

   The interfaces appear in the form *<circuit_name>.llc2*

3. **Change the setting of the Enable parameter, if necessary.**

   (Refer to the parameter description that follows this procedure.)

4. **Click on Apply to save your change.**

5. **Click on Done.**

   The Configuration Manager window reappears.

Following is a description of the parameters in the DLSw Interface Configuration window.

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables Data Link Switching over this interface. *Enable* — Initializes the DLSw interface you added to a physical circuit. Also use the Enable setting to reinitialize an existing DLSw interface disabled earlier. The state of the interface depends on the up/down state of the associated circuit and slot. *Disable* — Switches a DLSw interface from the enabled (up) state to the disabled (down) state.
Instructions:	Select Enable if you previously set this parameter to Disable and now want to re-enable Data Link Switching over this interface. Select Disable only if you want to disable Data Link Switching over this interface. This cancels all active LLC2 sessions currently supported by the interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.2.1.2

Enabling a DLSw Interface Using the Edit Circuits Function

You can also access the Enable parameter of a DLSw interface through the Edit Circuits function. To do so, begin at the Configuration Manager window (refer to Figure 5-1), and do either of the following:

- Select Circuits→Edit Circuits to bring up the Circuit List window (Figure 5-4); then select a circuit and click on Edit.
- Select a connector in the Configuration Manager window to invoke the Edit Connector window (Figure 5-5); then click on Edit Circuit.

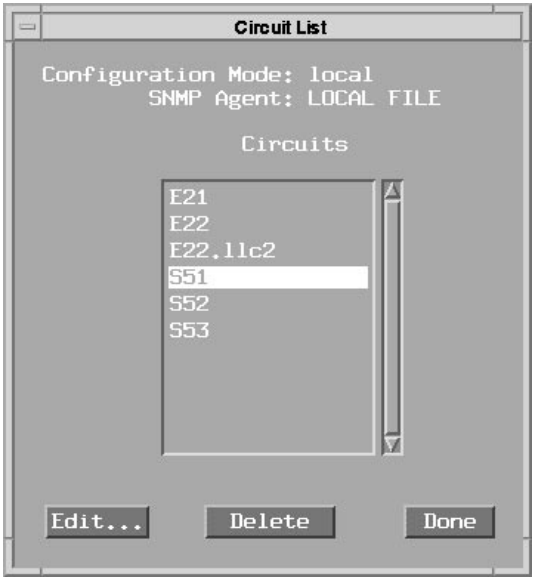


Figure 5-4. Circuit List Window

Figure 5-5. Edit Connector Window

In either case, the Circuit Definition window appears (Figure 5-6). Follow these steps to enable or disable a DLSw interface.

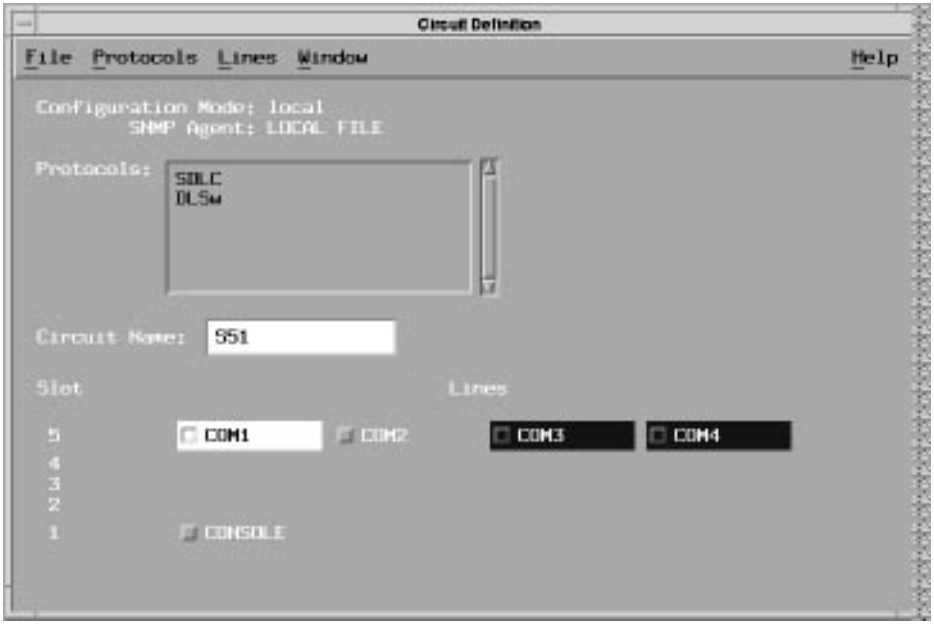


Figure 5-6. Circuit Definition Window

1. **Select Protocols→DLSw→Interfaces.**

   The Edit DLSw Interface window appears (Figure 5-7).

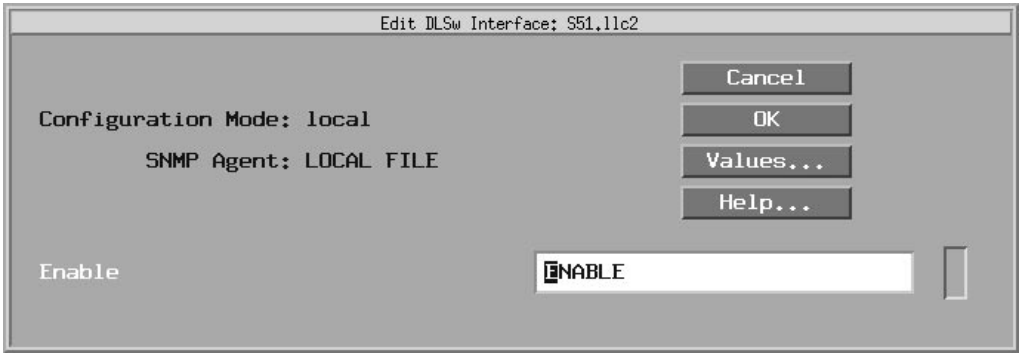


Figure 5-7. Edit DLSw Interface Window

2. **Click on Values and select Enable or Disable.**
3. **If you are editing an SDLC circuit, edit the Mode parameter by clicking on Values and selecting Primary or Secondary for the type of SDLC link station in this configuration.**
4. **Click on OK.**

   This closes the Edit DLSw Interface window, and the Circuit Definition window reappears (Figure 5-6).
5. **Select File→Exit.**

The result of Step 5 depends on how you originally accessed the DLSw Interface Enable parameter:

- If you selected Circuits→Edit Circuits from the Configuration Manager window, the Circuit List window appears (refer to Figure 5-4). Clicking on Done in the Circuit List window completes the procedure and returns you to the Configuration Manager window.
- If you selected a connector to invoke the Edit Connector window (refer to Figure 5-5), the Configuration Manager window appears, indicating that you completed the procedure.

Editing DLSw Peer IP Table Parameters

The DLSw Peer IP Table contains the list of all configured (remote) peers known to the local router. This section describes how to add, edit, and delete configured peers. (Refer to Chapter 3 for more information on configured and unconfigured peers.)

To access the DLSw Peer IP Table, begin at the Configuration Manager window (refer to Figure 5-1)and select Protocols→DLSw→Peer IP Table. The DLSw Peer Configuration window appears, listing all DLSw configured peers known to the local router (Figure 5-8).

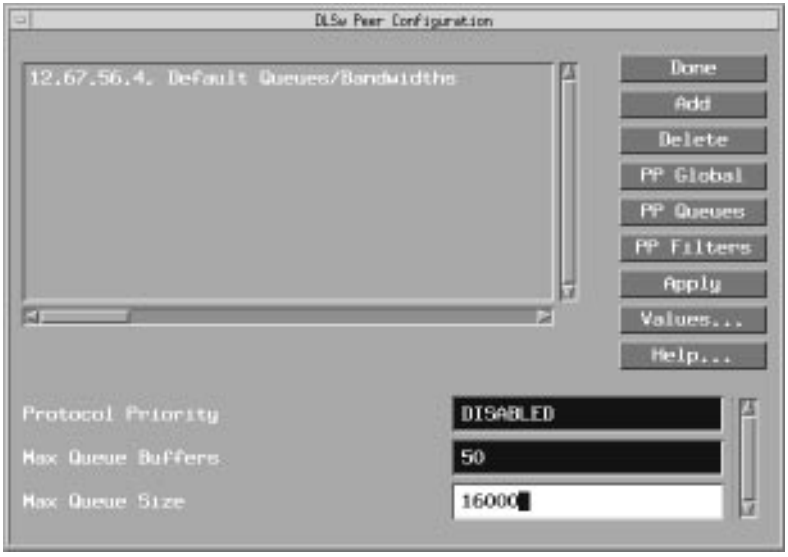


Figure 5-8. Configured Peer in DLSw Peer Configuration Window

Note: *The DLSw protocol prioritization and traffic filtering functions are described in Chapter 6. Refer to this chapter for information on the Protocol Priority, Max Queue Buffers, and Max Queue Size parameters, as well as information on the protocol priority buttons in the DLSw Peer Configuration window.*

Adding a DLSw Peer IP Table Entry

To add a new DLSw Peer IP Table entry, begin at the DLSw Peer Configuration window (refer to Figure 5-8) and then

1. **Click on Add.**

   The second DLSw Peer Configuration window appears (Figure 5-9).

2. **Type a value for the Peer IP Address parameter.**

Note: *Do not enter the IP address of any DLSw peer (slot) that resides in the local router.*

Figure 5-9. IP Address in DLSw Peer Configuration Window

3. **Click on OK.**

   This saves the new entry. The DLSw Peer Configuration window reappears (refer to Figure 5-8) with the new entry in the list of existing peers.

4. **Click on Done.**

   The Configuration Manager window reappears.

Parameter:	**Peer IP Address**
Default:	None
Options:	Any valid, 32-bit IP address in the form *network.host* (using dotted decimal notation)
Function:	Specifies the IP address of a remote DLSw peer. Adding this address to the DLSw IP Peer Table defines a configured peer to the local router. Configured peers receive all DLSw-related broadcast frames from the local router.
Instructions:	Type the IP address at which the configured peer should receive all DLSw-related broadcast frames.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.5.1.3

Editing a DLSw Peer IP Table Entry

You cannot edit the Peer IP Address parameter associated with an existing DLSw Peer IP Table entry. To change the IP address of an entry, proceed as follows:

1. **Delete the existing entry from the DLSw Peer IP Table.**

   (See the following section, “Deleting a DLSw Peer IP Table Entry.”)

2. **Using the appropriate IP address, add a new configured peer entry to the DLSw Peer IP Table.**

   (See the preceding section, “Adding a DLSw Peer IP Table Entry.”)

Deleting a DLSw Peer IP Table Entry

To delete a DLSw Peer IP Table entry, start at the DLSw Peer Configuration window (Figure 5-10):

1. **Select the entry to delete.**
2. **Click on Delete.**

Figure 5-10. Deleting a DLSw Peer IP Table Entry

The system software deletes the entry, and the entry disappears from the list of configured peers.

3. **Click on Done.**

   The Configuration Manager window reappears.

Editing the DLSw Slot IP Table

The DLSw Slot Configuration Table contains a list of all DLSw-capable slots in your router. Each table entry establishes a slot in the router as a DLSw peer on your TCP/IP network.

You identify a slot by its number in the router chassis, and a DLSw peer by its IP interface address on the TCP/IP network. DLSw Slot IP Table entries associate the number of a DLSw-capable slot with the IP network address of that (peer) slot. This section describes how to add, edit, and delete DLSw Slot IP Table entries.

Note: *Before you add any entries to the slot table, you must add/allocate one IP interface for each DLSw-capable slot in the router configuration. You need not configure the associated IP and DLSw interfaces on the same slot. You can also use the circuitless IP interface address for a DLSw-capable slot. Using the circuitless IP interface allows TCP connections for DLSw services on that slot to be less dependent on the availability of specific physical circuits or datalinks. (For more information on the nature and use of the circuitless IP interface, see* Configuring IP Services*.)*

To access the DLSw Slot IP Table, begin at the Configuration Manager window (refer to Figure 5-1) and select Protocols→DLSw→Slot IP Table. The DLSw Slot Configuration window appears, showing a list of all slots serving as DLSw peers on your TCP/IP network (Figure 5-11).

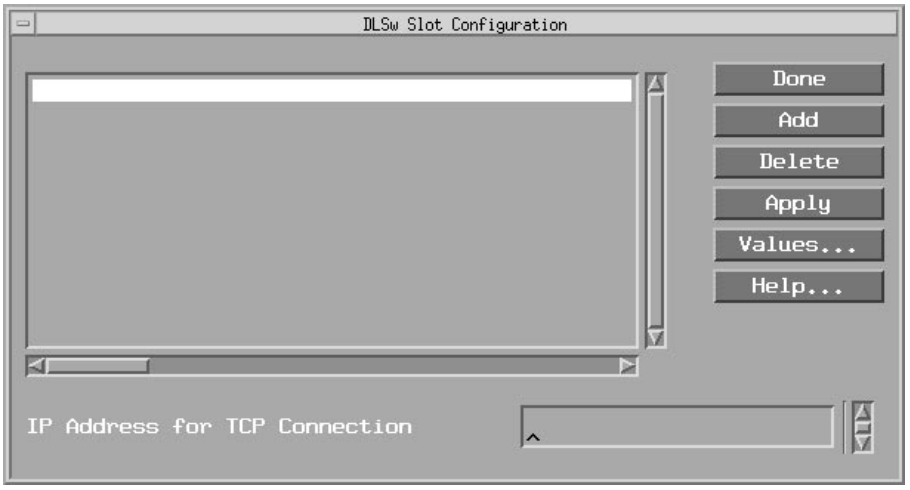


Figure 5-11. DLSw Slot Configuration Window

Adding a DLSw Slot IP Table Entry

To add a new DLSw Slot IP Table entry, begin at the DLSw Slot Configuration window (Figure 5-11) and then

1. **Click on Add.**

   The DLSw Slot Configuration window appears as shown in Figure 5-12.

Figure 5-12. IP Address in DLSw Slot Configuration Window

2. **Type a value for the Slot parameter.**
3. **Type the IP address of an interface configured earlier on the router.**

   Each DLSw-capable slot requires its own IP interface in the router configuration. Do not specify the same IP interface address for two or more different DLSw-capable slots in the same router configuration.
4. **Click on OK to save your entry to the configuration file.**

   The DLSw Slot Configuration window reappears (refer to Figure 5-11) with the new entry added to the list of existing DLSw-capable slots.

Following are descriptions of the DLSw Slot IP Table parameters.

Parameter:	**Slot**
Default:	None
Range:	1 to 14
Function:	Specifies the slot number you want to associate with the IP interface address you reserved for that slot.
Instructions:	Type a slot number from 1 to 14, depending on • Type of node/chassis • Slots that link modules can occupy
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.3.1.2

Parameter:	**IP Address**
Default:	None
Options:	Any valid, 32-bit IP address in the form *network.host* in dotted decimal notation
Function:	Specifies an IP address associated with a specific DLSw peer (slot) in the router. TCP uses this IP address for connections associated with that slot.
Instructions:	Type a valid IP address for the slot. The IP interface need not reside on the DLSw-capable slot. Do *not* enter a value for every active slot in the router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.3.1.3

Editing a DLSw Slot IP Table Entry

You can edit only the IP Address for TCP Connection parameter in an existing DLSw Slot IP Table entry.

To edit the IP address associated with a particular slot, begin at the Configuration Manager window (refer to Figure 5-1):

1. **Select Protocols→DLSw→Slot IP Table.**

   The DLSw Slot Configuration window appears (Figure 5-13).

2. **Select the DLSw Slot IP Table entry.**

3. **Click on the IP Address for TCP Connection parameter box, and enter a new IP address.**

4. **Click on Apply.**

   This saves your changes to the router configuration file.

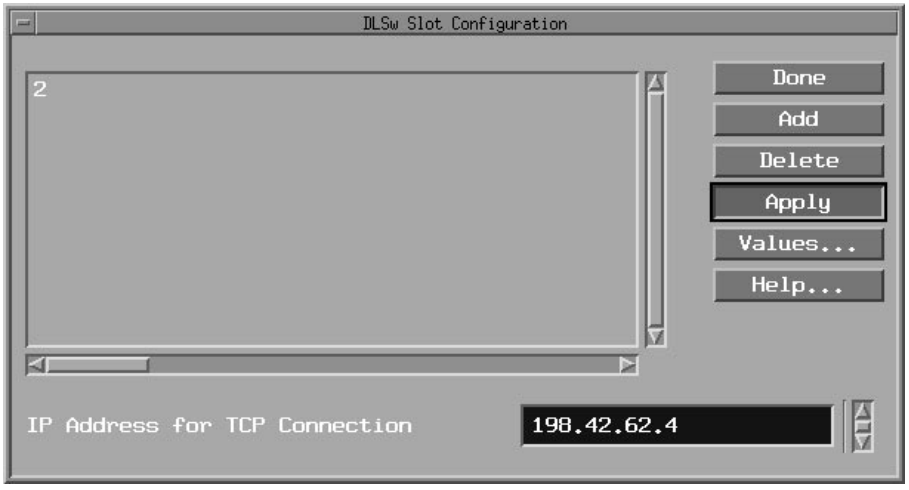


Figure 5-13. Saving an Edited DLSw Slot IP Address

5. **Click on Done.**

   The Configuration Manager window reappears.

Following is a description of the IP Address for TCP Connection parameter.

Parameter:	**IP Address for TCP Connection**
Default:	None
Options:	Any valid, 32-bit IP address in the form *network.host* in dotted decimal notation
Function:	Specifies an IP address associated with a specific DLSw peer (slot) in the router. TCP uses this IP address for connections associated with that slot.
Instructions:	Type a valid IP address for each slot. The IP interface need not reside on the DLSw-capable slot. Do *not* enter a value for every active slot in the router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.3.1.3

Deleting a DLSw Slot IP Table Entry

To delete a DLSw Slot IP Table entry, start at the DLSw Slot Configuration window (Figure 5-14):

1. **Select the Slot IP Table entry.**
2. **Click on Delete.**

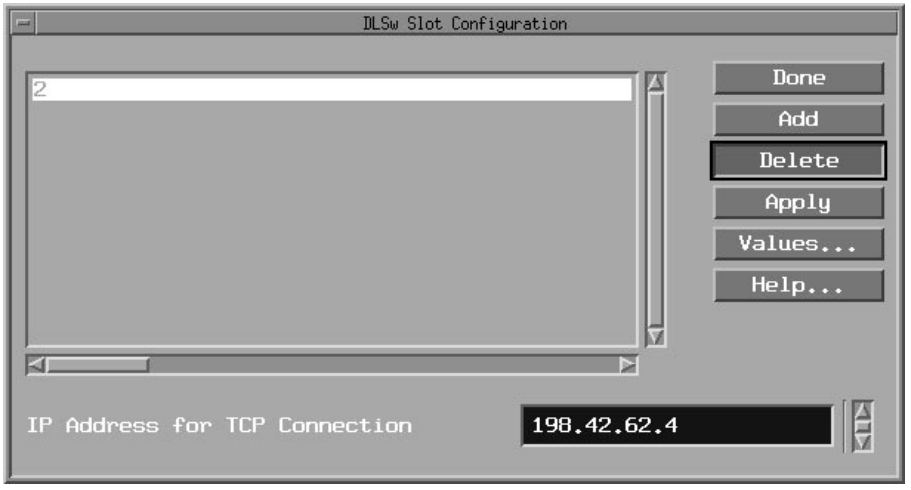


Figure 5-14. Deleting a DLSw Slot Table Entry

The system software deletes the entry you selected, and the entry disappears from the list of DLSw Slot IP Table entries in the DLSw Slot Configuration window.

3. **Click on Done.**

   You return to the Configuration Manager window.

Editing DLSw SAP Table Parameters

The DLSw SAP Table contains a list of the service access point (SAP) addresses associated with communication subsystems on PCs, hosts, FEPs, cluster controllers, and other systems in your network. This section describes how to add, edit, and delete DLSw SAPs.

Each SAP Table entry establishes a DLSw SAP address and a SAP window (flow control parameter) value for that SAP. (See Chapter 3 for more information on DLSw SAPs.)

DLSw SAP Table entries appear in the DLSw SAP Configuration window. When you add DLSw to a router configuration, there are four predefined SAP entries: 00, 04, 08, and 0C (Figure 5-15).

To access the DLSw SAP Configuration window, begin at the Configuration Manager window (refer to Figure 5-1) and select Protocols→DLSw→SAP Table. The DLSw SAP Configuration window appears (Figure 5-15), listing all SAP addresses that are accessible by means of DLSw services on the router.

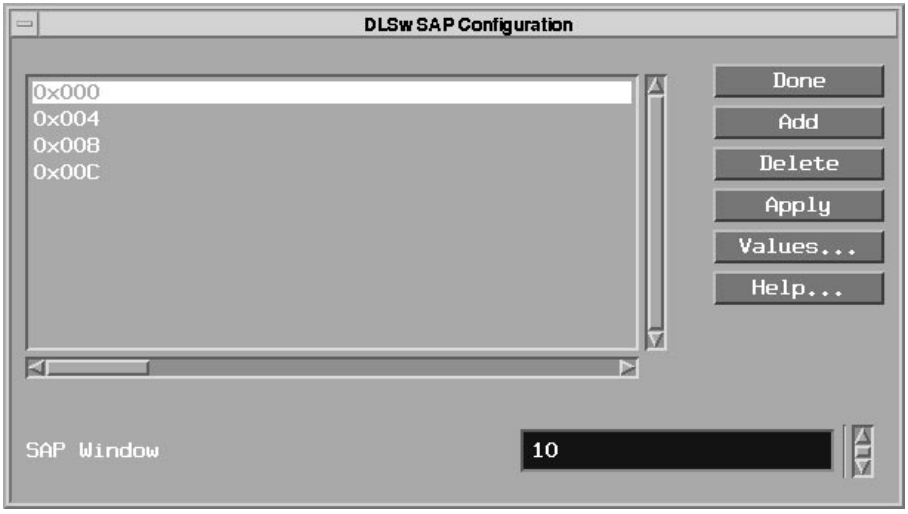


Figure 5-15. SAP Addresses in DLSw SAP Configuration Window

Adding a DLSw SAP Table Entry

To add a new SAP Table entry, begin at the DLSw SAP Configuration window (Figure 5-15) and

1. **Click on Add.**

   The DLSw SAP Configuration window appears as shown in Figure 5-16.

Figure 5-16. SAP Parameter in DLSw SAP Configuration Window

2. **Type the 0x prefix and then enter a hexadecimal value for the SAP parameter.**

   Valid SAP addresses include even values 00, 04 to EC, and F0.

3. **Click on OK.**

   This saves your entry to the router configuration file. The DLSw SAP Configuration window reappears (refer to Figure 5-15) with the new entry added to the list of existing DLSw SAPs.

4. **Repeat Steps 1 through 3 for each SAP you want to add.**

5. **Click on Done.**

   The Configuration Manager window reappears.

Following is a description of the SAP parameter.

Parameter:	**SAP**
Default:	None
Options:	An even-numbered SAP address (00, 04 to EC, F0) in hexadecimal format
Function:	Specifies the destination service access point (SAP) address associated with a communication subsystem on a remote device (for example, on a PC or host).
Instructions:	Begin the address with *0x* and type the SAP address associated with a specific communication subsystem. For example, the SAP associated with NetBIOS is 0xF0.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.4.1.2

Editing a DLSw SAP Table Entry

You can edit only the SAP Window (flow control) parameter associated with an existing DLSw SAP Table entry.

Note: *After you add an entry to the DLSw SAP Table, Site Manager disallows any attempt to edit the SAP address associated with that entry. To change the address of an existing DLSw SAP, you delete the entry in the DLSw SAP Configuration window, then add a new SAP with the new address. (Refer to the preceding section,* "Adding a DLSw SAP Table Entry," *for information about how to add a new DLSw SAP.)*

To edit the SAP Window parameter associated with a particular DLSw SAP, begin at the Configuration Manager window (refer to Figure 5-1):

1. **Select Protocols→DLSw→SAP Table.**

   The DLSw SAP Configuration window appears (Figure 5-17).

2. **Select the DLSw SAP Table entry to edit.**
3. **Click on the SAP Window parameter box and enter a new value.**
4. **Click on Apply.**

   This saves your changes (Figure 5-17).

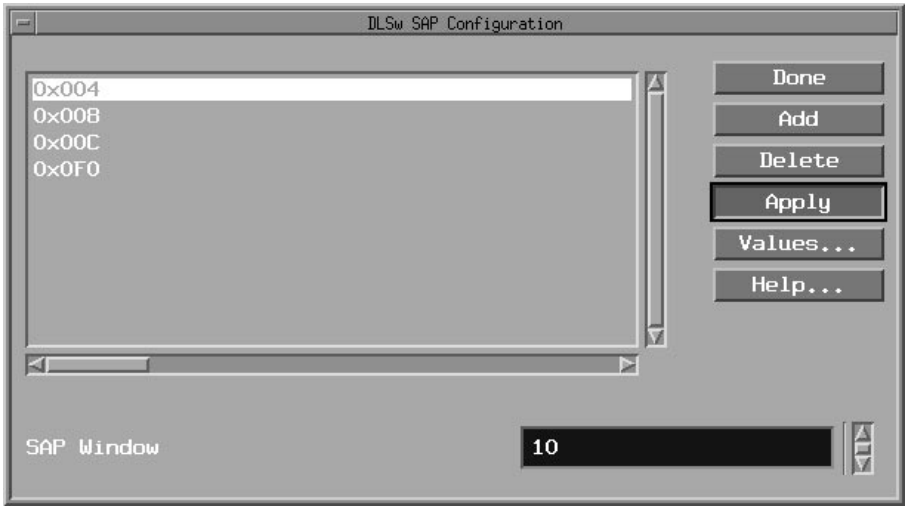


Figure 5-17. Saving the Edited SAP Window Setting

5. **Click on Done.**

   You return to the Configuration Manager window.

Following is a description of the SAP Window parameter.

Parameter:	**SAP Window**
Default:	10 (frames)
Range:	6 to 200 frames
Function:	Specifies the maximum number of unacknowledged LLC2 frames that the local endstation DLSw switch accepts for forwarding to the remote endstation. See the section “Flow Control” in Chapter 2 for more information.
Instructions:	Type a SAP window size that is appropriate for your network configuration and requirements. Specifying a larger size dedicates more buffer space to a particular SAP, thereby improving performance on that SAP. Specifying a smaller window size reduces buffer size and decreases performance on that SAP.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.4.1.3

.

Note: *The default value of 10 frames is based on the commonly used value of 7 frames plus additional frames to accommodate possible differences in timing between the router and the endstations.*

Deleting a DLSw SAP Table Entry

To delete a SAP table entry begin at the Configuration Manager window (refer to Figure 5-1):

1. **Select Protocols→DLSw→SAP Table.**

   This displays the DLSw SAP Configuration window (Figure 5-18).

2. **Select the SAP Table entry to delete.**

3. **Click on Delete.**

   The system software deletes the entry you selected, and the entry disappears from the DLSw SAP Configuration window.

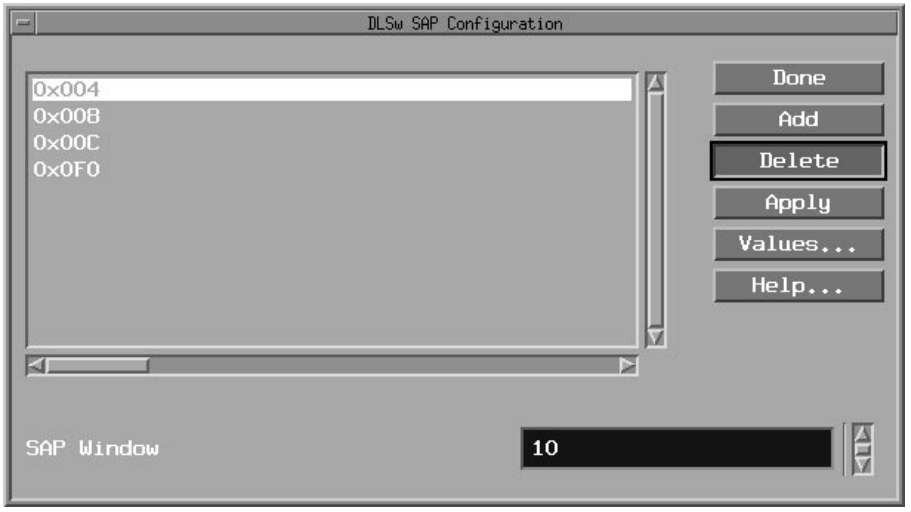


Figure 5-18. Deleting a SAP Table Entry

4. **Click on Done.**

   This completes the deletion procedure and returns you to the Configuration Manager window.

Editing DLSw Default NetBIOS Peer IP Table Parameters

The Default NetBIOS Peer IP Table contains the list of all remote NetBIOS systems and applications you can access via DLSw connection services on the local router. Each entry you define in the Default NetBIOS Peer IP Table associates the name of a NetBIOS client or server with the IP address of the remote DLSw peer that can reach that client or server. You add, edit, and delete Default NetBIOS Peer IP Table entries in the DLSw NetBIOS Peer Configuration window.

To access the DLSw NetBIOS Peer Configuration window, begin at the Configuration Manager window and select Protocols→DLSw→Default NetBIOS. The DLSw NetBIOS Peer Configuration window appears (Figure 5-19), showing a list of NetBIOS client and server names.

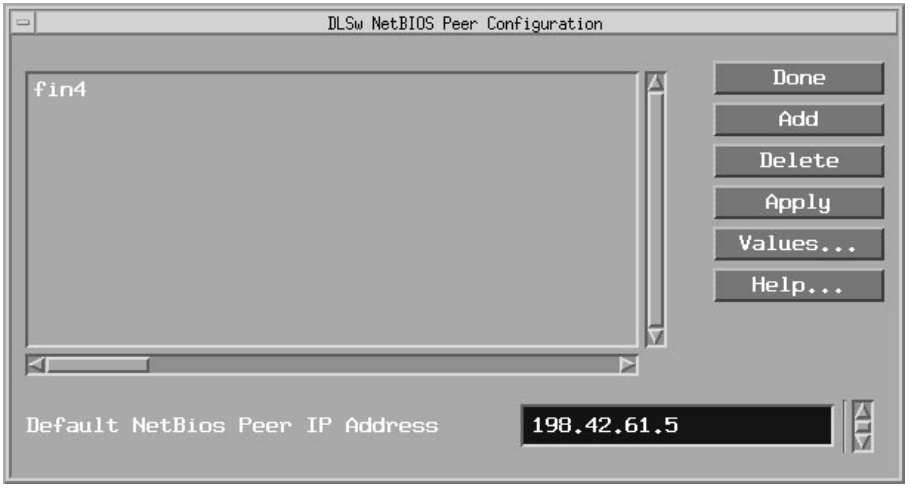


Figure 5-19. DLSw NetBIOS Peer Configuration Window

Clicking on a name in the list window causes the DLSw Peer IP address associated with that name to appear in the Default NetBIOS Peer IP Address parameter window (Figure 5-19).

Adding a DLSw Default NetBIOS Peer IP Table Entry

To add a new DLSw Default NetBIOS Peer IP Table entry, from the DLSw NetBIOS Peer Configuration window (Figure 5-19),

1. **Click on Add.**

   The DLSw NetBIOS Configuration window appears (Figure 5-20).

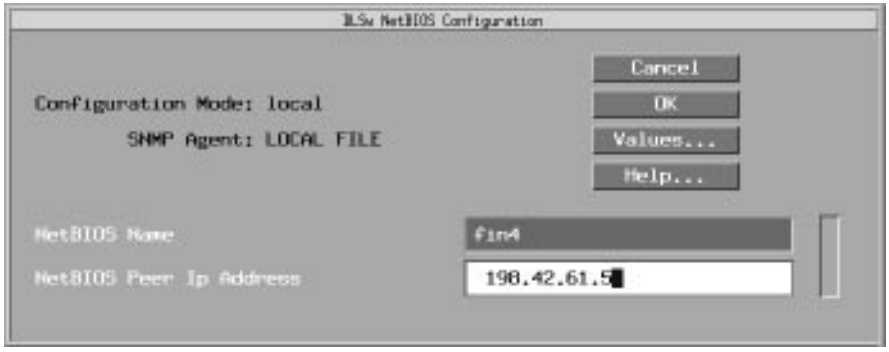


Figure 5-20. DLSw NetBIOS Configuration Window

2. **Type the name of the remote NetBIOS client or server.**

   This is the client or server you want to reach via DLSw services.

3. **Type the IP address of the remote DLSw peer.**

   This is the IP address of the DLSw peer that can reach the NetBIOS client or server you identified with the NetBIOS Name parameter.

4. **Click on OK.**

   This saves your entry to the router configuration file.

   The DLSw NetBIOS Peer Configuration window reappears with the new entry in the list of existing NetBIOS peers (refer to Figure 5-19).

Following are descriptions of the NetBIOS Name and NetBIOS Peer IP Address parameters.

Parameter:	**NetBIOS Name**
Default:	None
Options:	Any valid NetBIOS name
Function:	Specifies the name of the remote NetBIOS client/server or application you want to reach via DLSw services.
Instructions:	Enter the name of the remote NetBIOS client or server station or application you want to reach via DLSw services.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.11.1.2

Parameter:	**NetBIOS Peer IP Address**
Default:	None
Options:	Any valid, 32-bit IP address in the form *network.host* (using dotted decimal notation)
Function:	Specifies the IP address of the DLSw peer that can reach the remote NetBIOS client/server or application named in the same DLSw Default NetBIOS Peer IP Table entry.
Instructions:	Enter the IP address of the DLSw peer that can reach the remote client or server station or application named in the same DLSw Default NetBIOS Peer IP Table entry. The router adds this IP address to the list of configured peers in the local DLSw Peer IP Table.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.11.1.3

Editing a DLSw Default NetBIOS Peer IP Table Entry

You can edit only the Default NetBIOS Peer IP Address parameter in a Default NetBIOS Peer IP Table entry. To edit the parameter, begin at the Configuration Manager window (refer to Figure 5-1):

1. **Select Protocols→DLSw→Default NetBIOS.**

   The DLSw NetBIOS Peer Configuration window appears (Figure 5-21).

2. **Select the DLSw Default NetBIOS Peer IP Table entry to edit.**

3. **Click on the Default NetBIOS Peer IP Address parameter and enter a new address.**

4. **Click on Apply.**

   This saves your change to the router configuration file.

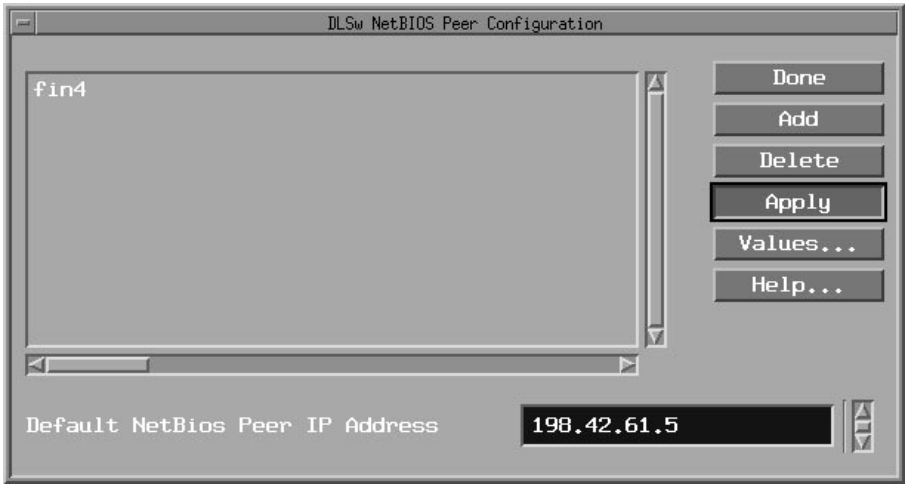


Figure 5-21. Saving a DLSw Default NetBIOS Peer IP Table Entry

5. **Click on Done.**

   You return to the Configuration Manager window.

Following is a description of the Default NetBIOS Peer IP Address parameter.

Parameter:	**Default NetBIOS Peer IP Address**
Default:	None
Options:	Any valid, 32-bit IP address in the form *network.host* (using dotted decimal notation)
Function:	Specifies the IP address of the remote DLSw peer that can reach the NetBIOS client/server system or application currently selected in the DLSw NetBIOS Peer Configuration window.
Instructions:	Type the IP address of the DLSw peer that can reach the remote client/server or application currently selected in the DLSw NetBIOS Peer Configuration window. The router adds this IP address to the list of configured peers in the local DLSw Peer IP Table.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.11.1.3

Deleting a DLSw Default NetBIOS Peer IP Table Entry

To delete a DLSw Default NetBIOS Peer IP Table entry from the router configuration, start at the DLSw NetBIOS Peer Configuration window (Figure 5-22):

1. **Select the table entry to delete.**

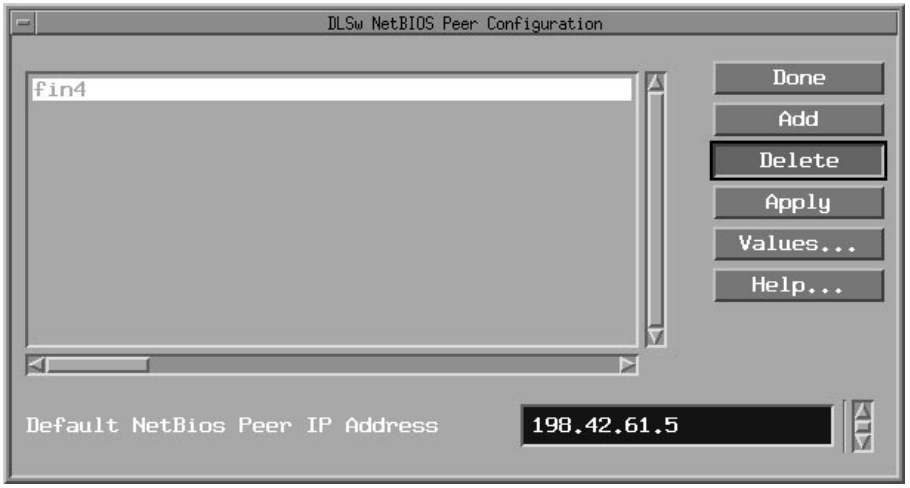


Figure 5-22. Deleting a DLSw Default NetBIOS Peer IP Table Entry

2. **Click on Delete.**

   The system deletes the entry you selected, and the entry disappears from the list.

3. **Click on Done.**

   You return to the Configuration Manager window.

Editing DLSw Default MAC Peer IP Table Parameters

The DLSw Default MAC Peer IP Table contains the list of all remote SNA systems and applications you can access via DLSw connection services on the local router. Each entry you define in the DLSw Default MAC Peer IP Table contains the IP address of a remote DLSw peer that can reach a target SNA system or application. The target system or application has an associated Token Ring/802.5 MAC address, which you also specify in the DLSw Default MAC Peer IP Table entry. You add, edit, and delete DLSw Default MAC Peer IP Table entries in the DLSw MAC Peer Configuration window.

To access the DLSw MAC Peer Configuration window, begin at the Configuration Manager window (refer to Figure 5-1) and select Protocols→DLSw→Default MAC.

The DLSw MAC Peer Configuration window appears (Figure 5-23), showing a list of Token Ring/802.5 MAC addresses associated with frequently accessed, remote SNA systems and applications.

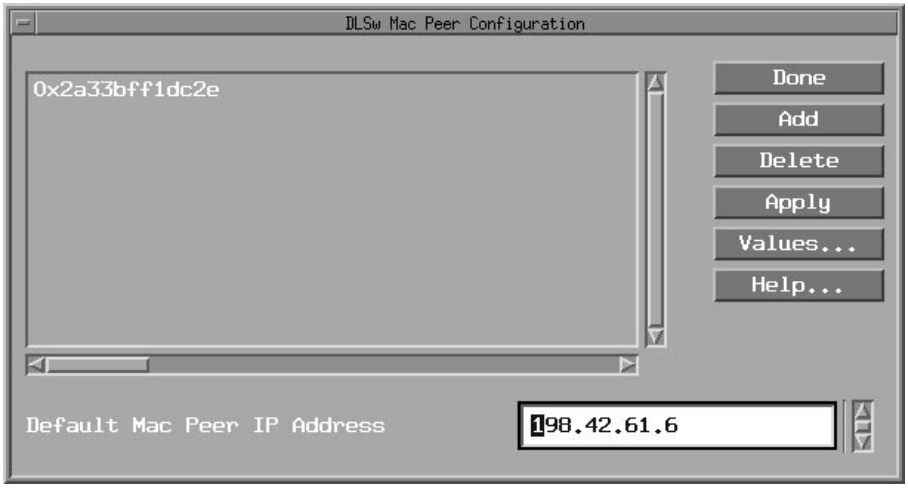


Figure 5-23. DLSw MAC Peer Configuration Window

Each entry in the list is associated with the IP address of the remote DLSw peer that can reach the target SNA system or application. The IP address of the currently selected table entry appears in the Default MAC Peer IP Address parameter box.

Adding a DLSw Default MAC Peer IP Table Entry

To add a new DLSw Default MAC Peer IP Table entry, begin at the DLSw MAC Peer Configuration window and

1. **Click on Add.**

   The DLSw MAC Configuration window appears (Figure 5-24).

Figure 5-24. MAC Addresses in the DLSw MAC Configuration Window

2. **Type the Token Ring/802.5 MAC address.**

   This is the address associated with the SNA system or application you want to reach via DLSw services.

3. **Type the IP address of the DLSw peer.**

   This is the IP address of the DLSw peer that can reach the SNA system or application you identified in the MAC Address parameter box.

4. **Click on OK.**

   This saves your entry to the configuration file.

   The DLSw MAC Peer Configuration window reappears with the new entry in the list of existing DLSw MAC peers (Figure 5-23).

Following are descriptions of the MAC Address and MAC Peer IP Address parameters.

Parameter:	**MAC Address**
Default:	None
Options:	Any valid, 48-bit MAC address expressed in hexadecimal notation
Function:	Specifies the MAC address associated with the SNA system or application you want to reach via DLSw services.
Instructions:	Type in hexadecimal format the MAC address associated with the remote SNA system or application you want to reach via DLSw services.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.10.1.2

Parameter:	**MAC Peer IP Address**
Default:	None
Options:	Any valid, 32-bit IP address in the form *network.host* (using dotted decimal notation)
Function:	Specifies the IP address of a remote DLSw peer that can reach the remote SNA system or application identified by the MAC address in the same Default MAC Peer IP Table entry. The router adds this IP address to the list of configured peers in the DLSw Peer IP Table.
Instructions:	Type the IP address of the remote DLSw peer that can reach the remote SNA system or application identified by the MAC address in the same Default MAC Peer IP table entry.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.10.1.3

Editing a DLSw Default MAC Peer IP Table Entry

You can edit only the Default MAC Peer IP Address parameter in the Default MAC Peer IP Table. To edit the DLSw MAC Peer IP Address, begin at the Configuration Manager window (refer to Figure 5-1):

1. **Select Protocols→DLSw→Default MAC.**

   The DLSw MAC Peer Configuration window appears (Figure 5-25).

2. **Select the entry to edit.**

3. **Click on the Default MAC Peer IP Address parameter window and enter a new address.**

4. **Click on Apply.**

   This saves your change to the router configuration file.

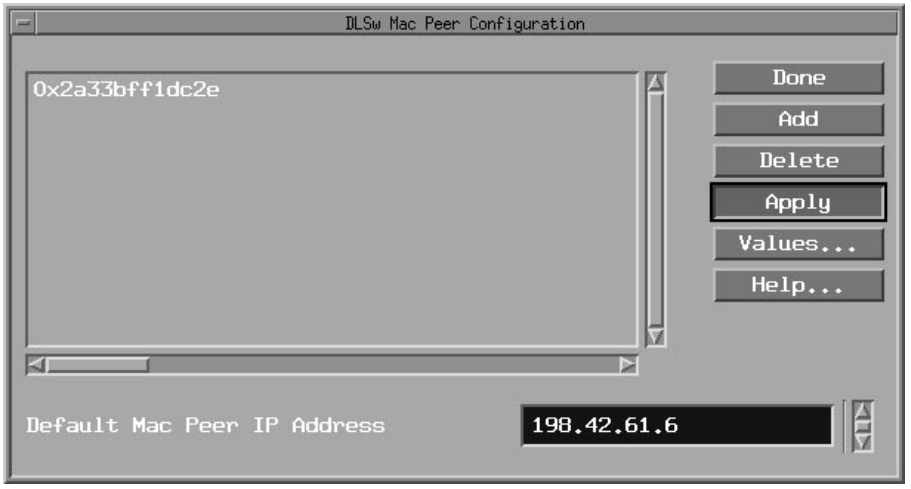


Figure 5-25. Saving a DLSw Default MAC Peer IP Table Entry

5. **Click on Done.**

   The Configuration Manager window reappears.

Following is a description of the Default MAC Peer IP Address parameter.

Parameter:	**Default MAC Peer IP Address**
Default:	None
Options:	Any valid, 32-bit IP address in the form *network.host* (using dotted decimal notation)
Function:	Specifies the IP address of a remote DLSw peer that can reach the SNA system or application identified by MAC address and currently selected in the DLSw MAC Peer Configuration window. The router adds this IP address to the list of configured peers in the DLSw Peer IP Table.
Instructions:	Type the IP address of the remote DLSw peer that can reach the remote SNA system or application identified by MAC address and currently selected in the DLSw MAC Peer Configuration window.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.10.1.3

Deleting a DLSw Default MAC Peer IP Table Entry

To delete a DLSw Default MAC Peer IP Table entry from the router configuration, start at the DLSw MAC Peer Configuration window (Figure 5-26):

1. **Select the entry to delete.**
2. **Click on Delete.**

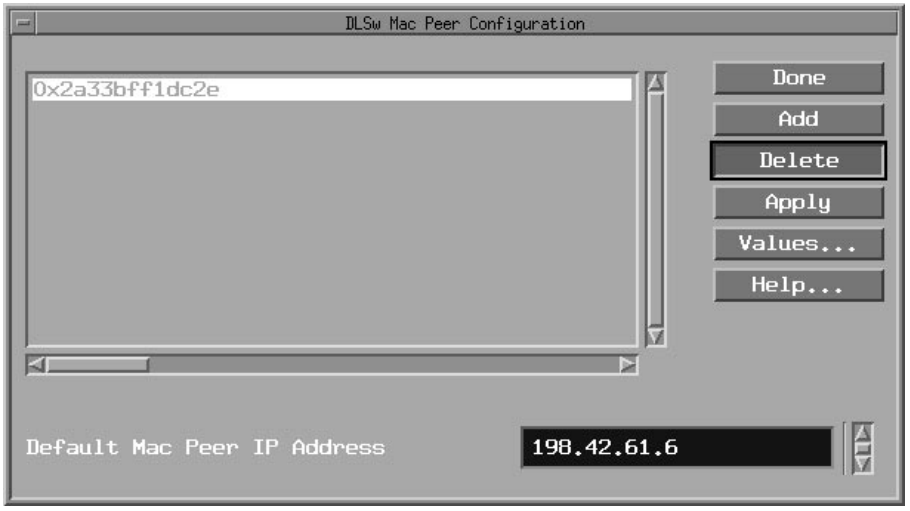


Figure 5-26. Deleting a DLSw Default MAC Peer IP Table Entry

The system software deletes the entry you select, and the entry disappears from the list.

3. **Click on Done.**

   The Configuration Manager window reappears.

Editing DLSw Local Devices Parameters

DLSw Local Devices parameters let you map SDLC devices to LAN MAC and SAP addresses. This section assumes that you have already added local devices. Chapter 3 describes the different ways that you can add local devices. You should read this section if you want to edit the local device configurations.

To access DLSw Local Devices parameters, begin at the Configuration Manager window (refer to Figure 5-1):

1. **Select Protocols→DLSw→Local Devices.**

   The DLS Local Device Configuration window appears (Figure 5-27).

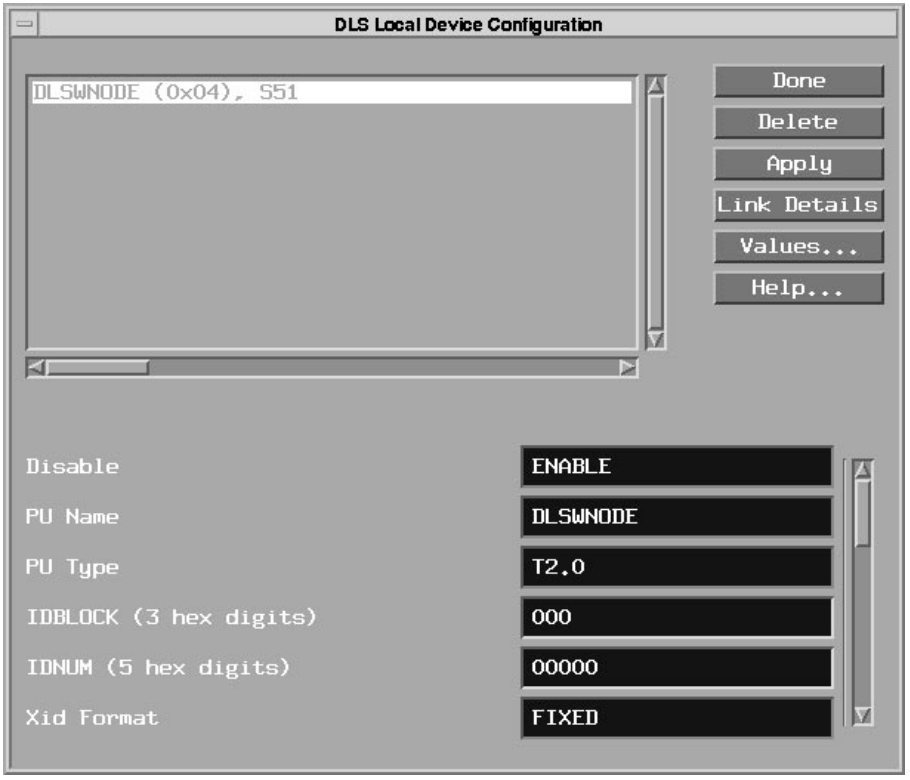


Figure 5-27. DLS Local Device Configuration Window

2. **Click on the local device whose parameters you want to change.**

   Edit the parameters you want to change. For information, see the next section, "DLSw Local Devices Parameter Descriptions."

3. **Click on Apply to save your changes.**

4. **Proceed as follows:**

   - To edit the parameters of another local device, select that device and repeat Steps 2 and 3.
   - Select Link Details to display the SDLC Link Station Configuration window. Refer to *Configuring SDLC Services* for information on the parameters in this window.

- To add a local device, start at the Configuration Manager window and select the connector to which you are adding a local device. Select Edit Circuit, then select the Protocols→DLSw→Local Devices menu path. The DLS Local Device Configuration window (Figure 5-28) appears with the Add button.

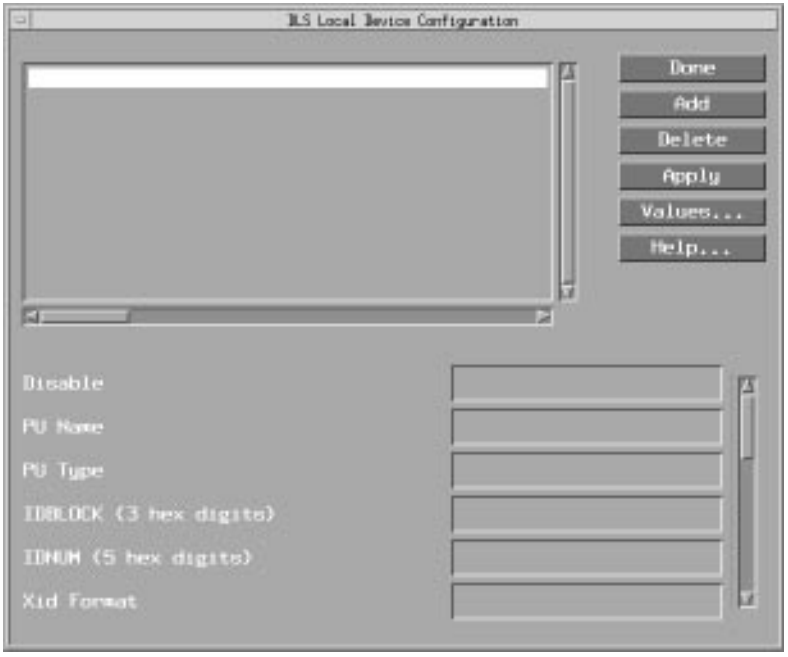


Figure 5-28. DLS Local Device Configuration Add Window

- If you are finished working with the local device parameters, click on Done to return to the Configuration Manager window.

DLSw Local Devices Parameter Descriptions

This section describes the DLSw Local Devices parameters you can customize from the DLS Local Device Configuration window.

Parameter:	**Link Address (hex)**
Default:	None
Options:	Any valid hexadecimal link station address from 0x01 to 0xFE
Function:	Specifies the address of the link station.
Instructions:	Type 0x followed by the link station address.
MIB Object ID:	N/A

Parameter:	**Disable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables the DLSw local device.
Instructions:	Set to Disable if you want to temporarily disable the local device, rather than delete it. Set to Enable if you want to reinitialize the local device.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.2

Parameter:	**PU Name**
Default:	None
Options:	Any valid, 8-byte ASCII name
Function:	Specifies the name of the adjacent link station. This name uniquely identifies the station for statistics and Alert messages.
Instructions:	Type the 8-byte ASCII link station name.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.7.5.1.32

Parameter:	**PU Type**
Default:	None
Options:	T2.0 | T2.1
Function:	Specifies the type of the XID-sending node. This parameter is used with the IDBLOCK, IDNUM, and XID Format parameters to determine the station exchange identification (XID) value.
Instructions:	Choose either T2.0 or T2.1.
MIB Object ID:	N/A

Parameter:	**IDBLOCK**
Default:	None
Options:	017 | 061 | any other 3-digit hexadecimal value
Function:	Specifies the block number, which must match the host's IDBLOCK parameter value that identifies incoming connection requests. This parameter is used with the PU Type, IDNUM, and XID Format parameters to determine the station exchange identification (XID) value.
Instructions:	Obtain the configured value at the host (from VTAM or other host operating system) for this device. In most cases: — Type 017 for a 3174 in T2.0 mode. — Type 061 for a T2.0 node in fixed format.
MIB Object ID:	N/A

Parameter:	**IDNUM**
Default:	None
Options:	Any 5-digit hexadecimal value from 00000 to FFFFF (for T2.0 nodes)
Function:	Specifies the ID number, which must match the host's IDNUM parameter value that identifies incoming connection requests. This parameter is used with the PU Type, IDBLOCK, and XID Format parameters to determine the station exchange identification (XID) value.
Instructions:	Obtain the configured value at the host (from VTAM or other host operating system) for this device. Type a 5-digit hexadecimal value from 00000 to FFFFF for T2.0 nodes.
MIB Object ID:	N/A

Parameter:	**XID Format**
Default:	None
Options:	FIXED | VARIABLE1 | VARIABLE2
Function:	Specifies the format of the XID I-field.
Instructions:	Click on Values and select one of the following options: FIXED Fixed format (for T2.0) VARIABLE1 Variable format (for T1/T2.0/T2.1 to T4/T5 node exchanges) VARIABLE2 Variable format (for T2.1 to T2.1/T4/T5 node exchanges)
MIB Object ID:	N/A

Parameter:	**Source (Virtual) MAC (hex)**
Default:	None
Options:	Any standard MSB Token Ring MAC address
Function:	Specifies the source MAC address of an emulated Token Ring endstation for this device.
Instructions:	Type the 12-digit hexadecimal source MAC address you want to assign to the SDLC device. The address should be in MSB format, and it should be unique in the network (even among other source addresses on the router).
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.6

Parameter:	**Source (Virtual) SAP (hex)**
Default:	0x4
Range:	0x01 to 0xFE
Function:	Specifies the source service access point (SAP) of an emulated Token Ring or Ethernet endstation for this device.
Instructions:	Begin the address with *0x* and type a 1-digit or 2-digit hexadecimal source SAP address associated with this device. Typical values are multiples of 4.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.7

Parameter:	**Destination (Host) MAC (hex)**
Default:	None
Options:	Any standard MSB Token Ring MAC address
Function:	Identifies (with the Destination SAP) the Token Ring or Ethernet host the local device will reach via SDLC services.
Instructions:	Consult your host system manager for the host MAC address; then type the 12-digit hexadecimal address.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.8

Parameter:	**Destination (Host) SAP (hex)**
Default:	0x4
Range:	0x01 to 0xFE
Function:	Identifies (with the Destination MAC) the Token Ring or Ethernet host the local device will reach via SDLC services.
Instructions:	Consult your host system manager for the host SAP address. Type *0x* followed by a 1-digit or 2-digit hexadecimal address.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.9

Parameter:	**MAXOUT**
Default:	7
Range:	1 to 127
Function:	Controls the maximum number of consecutive frames that an SDLC link station can send without acknowledgment.
Instructions:	Type a value from 1 to 127.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.7.5.1.10

Parameter:	**MAXDATA**
Default:	2057
Options:	265 | 521 | 1033 | 2057
Function:	Specifies the maximum frame size SDLC supports. This value includes the Transmission Header (TH) and Request Header (RH).
Instructions:	Enter a maximum frame size that is equal to or larger than the largest frame size that will be received.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.7.5.1.7

Parameter:	**Canureach Timer**
Default:	30 s
Range:	0 to 3600
Function:	Specifies the time interval (in seconds) after which the router sends a canureach message to the remote DLSw peer to establish a session.
Instructions:	Enter the number of seconds you want for the time interval. For example, type a 1 to transmit a canureach message once per second, or type 3600 to transmit the message once per hour. Type a 0 if you do not want to transmit a canureach message.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.11

Parameter:	**Canureach Retries**
Default:	4294967295
Range:	0 to 4294967295
Function:	Specifies the number of times a canureach message is sent to the remote DLSw peer to establish a session.
Instructions:	Type the number of retries you want. Type a 0 if you do not want to transmit canureach messages. Leave the default value 4294967295 to send an infinite number of canureach messages for this connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.12

Parameter:	**Link Station Timer**
Default:	30 s
Range:	0 to 3600
Function:	Sets the time interval (in seconds) after which the router sends a connect request to the local SDLC device to establish a session.
Instructions:	Enter the number of seconds you want for the time interval. For example, type a 1 to send a connect request once a second, or type 3600 to send a connect request once an hour. Type a 0 if you do not want to send connect requests.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.13

Parameter:	**Link Station Retries**
Default:	4294967295
Range:	0 to 4294967295
Function:	Specifies the maximum number of times that a connect request is sent to the local SDLC device to establish a session.
Instructions:	Enter the number of retries you want. Type a 0 if you do not want to send connect requests. Leave the default value 4294967295 to send an infinite number of connect requests for this connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.14

Parameter:	**SDLC Receive Credit**
Default:	10
Range:	0 to 200
Function:	Specifies the maximum number of frames SDLC can send to DLSw. This is a flow control parameter.
Instructions:	Enter the maximum number of frames you want SDLC to send to DLSw. For example, type a 1 if you want DLSw to accept 1 frame from SDLC before it updates the SDLC credit. Type a 0 if you want DLSw to receive an infinite number of frames from SDLC without updating the SDLC credit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.15

Parameter:	**SDLC Transmit Credit**
Default:	10
Range:	0 to 200
Function:	Specifies the maximum number of frames DLSw can send to SDLC.
Instructions:	Enter the maximum number of frames you want DLSw to send to SDLC. For example, type a 1 if you want DLSw to send only one frame to SDLC until it receives credit update from SDLC. Type a 0 if you want DLSw to send an infinite number of frames to SDLC without updating the SDLC credit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.12.1.16

Deleting a DLSw Local Device Entry

To delete a DLSw Local Device entry from the router configuration, start at the DLS Local Device Configuration window (Figure 5-27):

1. **Select the DLSw local device to delete.**
2. **Click on Delete.**

Editing DLSw Traffic Filters and Protocol Prioritization

For information on how to access and configure traffic filters and protocol prioritization for DLSw services, refer to Chapter 6.

Deleting DLSw from the Node

You can delete DLSw from the node entirely.

To delete DLSw, begin at the Configuration Manager window (refer to Figure 5-1) and

1. **Select Protocols→DLSw→Delete DLS.**

   A confirmation window appears.

2. **Click on OK.**

   The Configuration Manager window appears.

DLSw is no longer configured on the router.

Chapter 6
Using DLSw Prioritization

This chapter provides guidelines for implementing Data Link Switching (DLSw) TCP-level Prioritization. Following an overview of DLSw protocol prioritization, later sections describe how to use Configuration Manager to

- Configure priority queues that apply to all configured or unconfigured DLSw peers (*default queues*)
- Configure priority queues that apply to individual configured DLSw peers (*peer-specific queues*)
- Create outbound traffic filters that process DLSw traffic into priority queues

Note: *The steps in this chapter assume that DLSw is already configured on an interface and that the Peer Table is complete. For information about configuring a circuit with DLSw and setting the slot, peer, and SAP parameters, refer to the earlier chapters in this manual.*

Protocol Prioritization Overview

Outbound traffic filters act on packets that the router sends out a synchronous interface to a wide area network. Outbound traffic filter actions let you direct traffic into delivery queues of varying precedence. Applying a priority queue action to an outbound filter is called *protocol prioritization*. These outbound filters are often called *priority filters*.

As a router operates, network traffic from a variety of sources converges at an interface. Without protocol prioritization, the router transmits packets in a first-in/first-out (FIFO) order. Site Manager's Protocol Prioritization features allow you to instruct the router to use a different transmit order for specified ranges of packets on an individual interface.

With protocol prioritization, the router sorts traffic into queues according to priority filters that you configure. For most traffic, you configure priority filters on an outbound interface. If a queue is full or you have configured an outbound drop filter, the router discards (*clips*) the traffic. For DLSw traffic you can also create priority queues for DLSw peers; the router cannot clip DLSw traffic.

The router holds the sorted packets in priority queues. It then uses a dequeuing allocation algorithm to drain the queues and transmit traffic.

Priority queues do not affect traffic as it is entering the router, but rather affects the sequence in which data leaves an interface. For this reason, Protocol Prioritization is considered an "outbound" filter mechanism.

Two Types of Protocol Prioritization

There are two separate implementations of protocol priority queuing. For all synchronous protocols that support outbound traffic filters, Bay Networks supports a high, normal, and low priority queue at the circuit interface level. For inbound and outbound DLSw traffic, Bay Networks also supports one to ten queues at the TCP level for DLSw peers.

Using existing protocol prioritization support, you can prioritize DLSw traffic before other protocols. DLSw protocol prioritization provides a mechanism for prioritizing specific types of DLSw traffic, such as:

- Ethernet
- Frame Relay
- SDLC
- Token Ring
- Other source route bridge (SRB) traffic

Note: *You can apply both circuit-level prioritization and TCP-level prioritization to DLSw traffic. Note that TCP-level prioritization alone does not give DLSw traffic precedence over other routing protocols. For information about circuit-level prioritization, refer to* Configuring Traffic Filters and Protocol Prioritization.

DLSw Priority Queues

This section describes how DLSw protocol prioritization works, and defines DLSw terms.

Although similar to the existing circuit-level protocol prioritization, DLSw prioritization is not limited to synchronous interfaces and does not operate at the driver level. DLSw prioritization occurs before TCP sequences packets, where the Data Link Control (LLC2 or SDLC) and TCP function.

The router sorts packets into priority queues as described in "The Enqueuing Process." The router then drains (*dequeues*) the priority queues to transmit packets according to a weighted allocation algorithm described in "The Dequeuing Process."

Based on the needs of your site, you can configure up to 10 queues for each DLSw peer. You can create queues for traffic with specific MAC or SAP address ranges or, for SNA traffic, based on criteria in the SNA Transmission Header (FID2 and FID4). You determine whether a queue applies to all DLSw peers or to one or more specific configured peer.

Default and Peer-Specific DLSw Queues

To set the way the router handles priority queues for *all* DLSw traffic (including unconfigured peers), you use the default DLSw queue configuration. To customize the handling of queued traffic for a *particular* configured peer, you configure peer-specific priority queues that apply to that peer's IP address only.

The default priority queue configuration applies to all configured DLSw peers *except* those individual peers for which you configure a custom priority queue. When you create peer-specific queues, they take precedence over the default queue.

The Enqueuing Process

The router enqueues packets that match a DLSw priority filter as follows:

1. Applies filter rules.
2. Stamps packets with a queue number.
3. Places packets in appropriate queues.

The router holds packets in the assigned priority queue according to how you configure DLSw protocol prioritization.

Based on the needs of your site, you can configure up to 10 queues (Queue 0 to Queue 9) for each DLSw peer. For example, you could assign a separate queue for each filter criterion, for specific address ranges, or for particular DLSw peers.

When you enable DLSw protocol prioritization, you distribute the available bandwidth for a configured DLSw peer among its priority queues. The combined bandwidth of each peer's queues totals 100 percent.

By default, there are two DLSw priority queues: Queue 0 receives 60 percent of the bandwidth and Queue 1 receives 40 percent.

Nonordered Queues

Although Site Manager numbers the DLSw priority queues, the queue number hierarchy does not determine priority. You configure both the number of queues for each DLSw peer and the percentage of bandwidth assigned to each queue. For example, you could assign 50 percent of available bandwidth to Queue 3 and 25 percent each to Queues 1 and 0.

The Dequeuing Process

The algorithm for DLSw bandwidth allocation is called *weighted dequeuing*. With weighted dequeuing, packets at the front of the protocol prioritization queues enter a *dequeue list* and receive a weighted score. Packets with the lowest score are transmitted first.

By distributing the selection of packets from all queues, weighted dequeuing generates less jitter than the round-robin algorithms used for circuit-level WAN protocol prioritization.

One goal of weighted dequeuing is to send smaller packets ahead of large packets, without violating the bandwidth of each queue or starving large packets. The algorithm accomplishes this by putting smaller packets ahead of larger packets by simultaneously considering how long the larger packets have been in the dequeue list. A large packet accumulates credit (lowering its weighted score) as each smaller packet gets ahead of it, and eventually the larger packet moves to the front of the dequeue list.

The Dequeue List

Three factors determine a packet's weighted score:

- Size of the packet
- Percent of bandwidth allocated to the packet's queue
- Time spent in the dequeue list

The dequeuing algorithm calculates a packet's dequeue weight using the following formula:

$$\text{Weight} = \frac{\text{Size of packet}}{\text{Bandwidth \%}} - \text{Time in dequeue list}$$

Weighted Dequeuing Algorithm

Weighted dequeuing works as follows:

1. Each priority queue enters its first (oldest) entry on a dequeue list.
2. The dequeue list orders the packets according to a weighted score.
3. TCP requests DLSw packets.
4. The router sends the requested number of packets or bytes to TCP from the top of the dequeue list, up to the configured queue limit.
5. TCP transmits the packets.
6. The sequence repeats at Step 1.

Figure 6-1 illustrates weighted dequeuing.

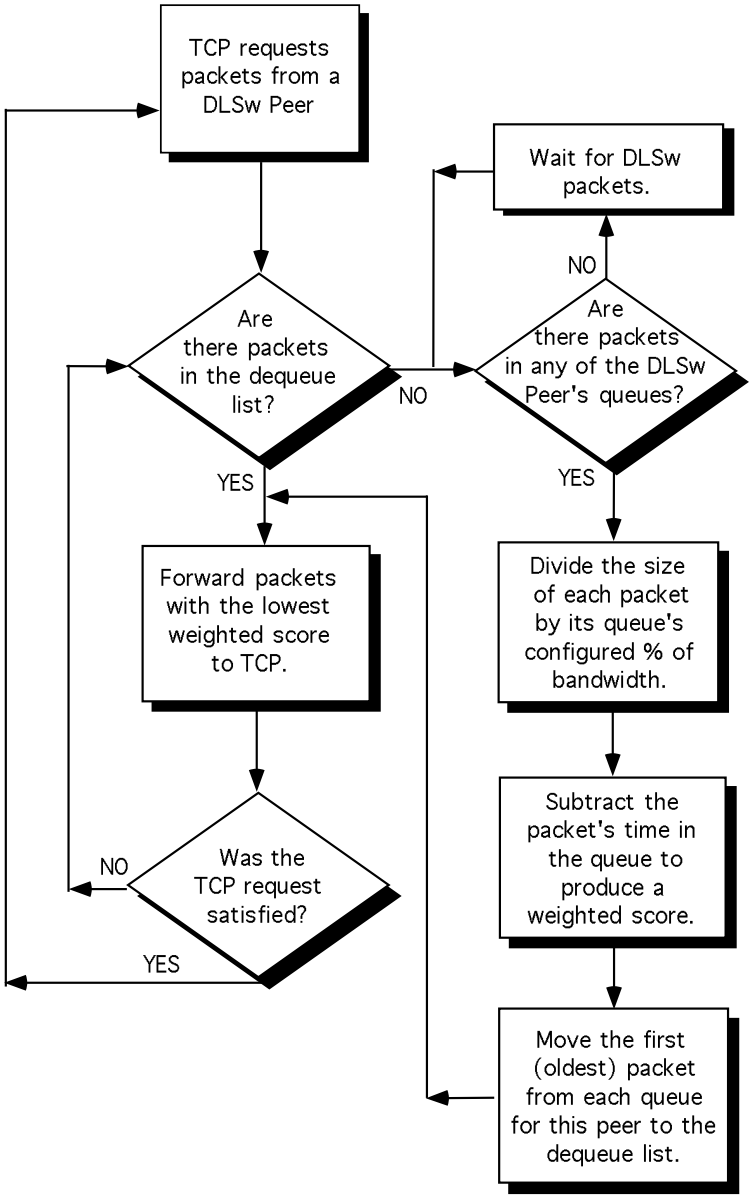

TCP requests packets from a DLSw Peer
Are there packets in the dequeue list?
NO
YES
Forward packets with the lowest weighted score to TCP.
Was the TCP request satisfied?
NO
YES
Are there packets in any of the DLSw Peer's queues?
NO
YES
Wait for DLSw packets.
Divide the size of each packet by its queue's configured % of bandwidth.
Subtract the packet's time in the queue to produce a weighted score.
Move the first (oldest) packet from each queue for this peer to the dequeue list.

Figure 6-1. Weighted Bandwidth Allocation

Tuning DLSw Protocol Prioritization

This section explains how congestion control and queue depth affect DLSw prioritization results for your network. The sections “Customizing the Default Queue Configuration” and “Customizing Specific DLSw Peer Queues” later in this chapter show how to use Configuration Manager to configure these values.

DLSw Priority Queues and Congestion Control

Because the router cannot clip DLSw traffic without breaking the DLSw session, DLSw protocol prioritization includes an internal congestion control feature to

- Temporarily save overflow packets in memory until the appropriate priority queue can handle them
- Notify DLSw to stop and start the flow of packets

There must be sufficient memory available to congestion control to prevent clipping. The less the congestion, the better the queue performance.

Queue Depth

Using Site Manager parameters, you configure the maximum queue buffers and the percentage of bandwidth for each queue.

Queue depth is the configurable number of packets that each DLSw priority queue can hold. The default value is 50 packets, regardless of packet size.

When you set the queue depth, you assign buffers (which hold the packets) to the DLSw queues. To determine whether there are enough buffers for the DLSw traffic flow on your network, examine the following two protocol prioritization statistics which the router keeps for each DLSw priority queue:

- DLSw HiWater Packets Mark — The greatest number of packets that have been in each queue.
- DLSw Congestion Control Count — The number of packets the router has discarded from each queue. (The router discards packets from full priority queues.)

Generally, if a queue’s Congestion Control Count is high, and its HiWater Packets Mark is close to or equal to its queue depth, you have not assigned enough buffers to that queue.

Configuring Default Priority Queues

You configure the default behavior of DLSw protocol prioritization using the Global DLSw PP Parameters/Defaults window. Use this window to enable, disable, or change the default configuration of priority queues for configured and unconfigured DLSw peers.

This section shows how to

- Enable the default priority queues for all configured DLSw peers
- Enable the default priority queues for unconfigured peers
- Customize the default priority queue configuration

Note: *The steps in this section assume that DLSw is already configured on an interface and that the Peer Table is complete. For information about configuring a circuit with DLSw and setting the slot, peer, and SAP parameters, refer to earlier chapters.*

Enabling the Default Queues for Configured and Unconfigured Peers

Begin by displaying the DLSw Protocol Prioritization (PP) Global Parameters window.

1. **From the Configuration Manager window, select Protocols→DLSw→Prot Prioritization (Outbound)→Global (see Figure 6-2).**

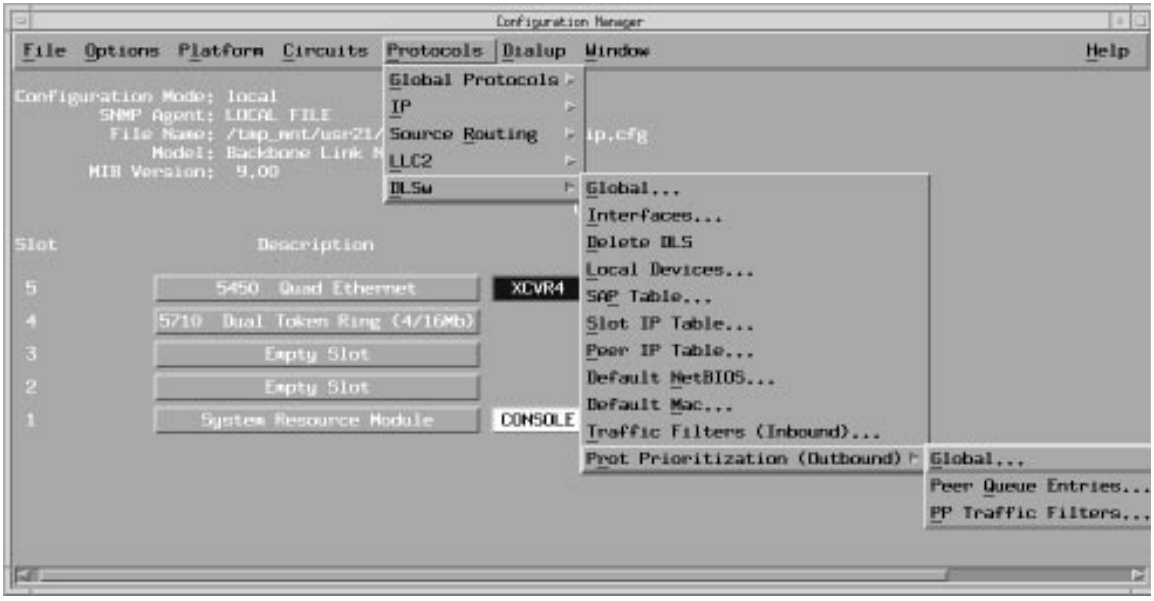


Figure 6-2. Selecting DLSw Protocol Prioritization

The Global DLSw PP Parameters/Defaults window appears (Figure 6-3).

Note: *See the section* "Using the DLSw Peer Configuration Window" *near the end of this chapter for another way to access the Global DLSw PP Parameters/Defaults window.*

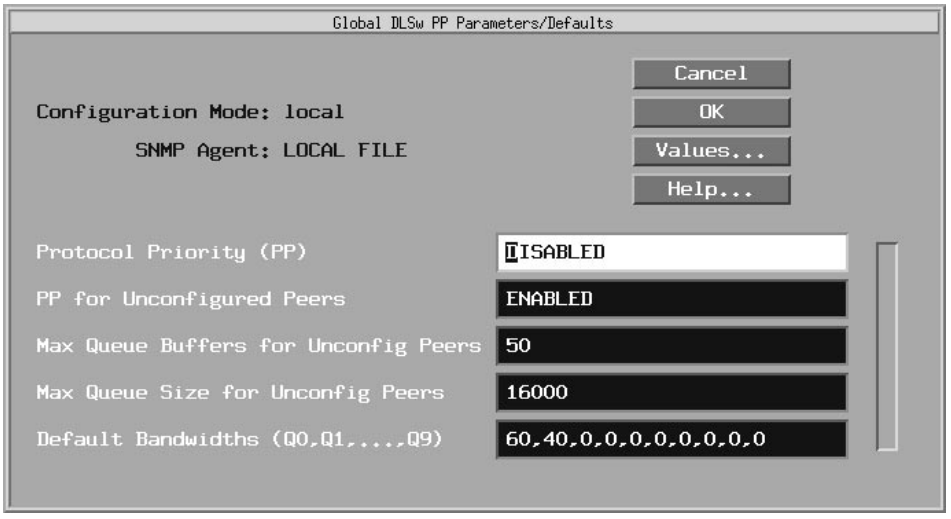


Figure 6-3. Global DLSw PP Parameters/Defaults Window

2. **Select Protocol Priority (PP) and click on Values.**

   The Protocol Priority (PP) Values Selection window appears (Figure 6-4).

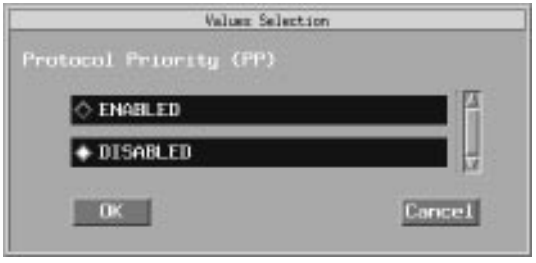


Figure 6-4. Enabling Protocol Prioritization on DLSw Peers

3. **Select ENABLED.**
4. **Click on OK.**

   The Global DLSw PP Parameters/Defaults window reappears (Figure 6-3).

5. **To also use the default priority queue structure for all *un*configured peers, change the value of the "PP for Unconfigured Peers" box to ENABLED (Figure 6-5).**

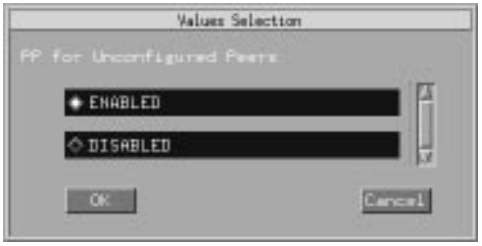


Figure 6-5. Enabling PP for Unconfigured Peers

6. **Click on OK.**

   The Global DLSw PP Parameters/Defaults window reappears (refer to Figure 6-3).

7. **Decide whether to use the default queue configuration or customize the queue to suit your network.**

8. **To use the default queue configuration, click on OK to exit.**

   Site Manager asks you to confirm (Figure 6-6).

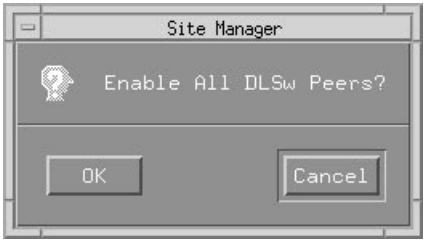


Figure 6-6. Enabling Protocol Prioritization for All DLSw Peers

9. **To customize the default queue configuration, continue with the next section, "Customizing the Default Queue Configuration."**

Customizing the Default Queue Configuration

Once you enable DLSw protocol prioritization, any DLSw peer uses default values that control how priority queues work. You can change these values according to your network traffic needs.

Note: *The default priority queue configuration applies to all configured DLSw peers* except *those configured with a custom priority queue configuration. Peer-specific queue configurations take precedence over the default DLSw priority queue configuration.*

Complete the following steps to edit the default DLSw protocol prioritization parameters:

1. **From the Configuration Manager window, select Protocols→DLSw→ Prot Prioritization (Outbound)→Global (refer to Figure 6-2).**

   The Global DLSw PP Parameters/Defaults window (Figure 6-7) appears.

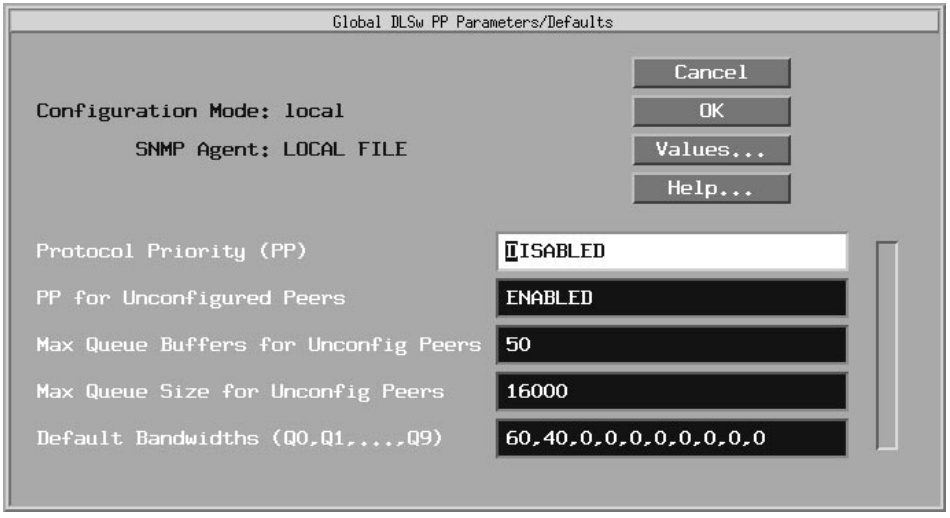


Figure 6-7. Global DLSw PP Parameters/Defaults Window

2. **Edit the parameters you want to change, using the descriptions following this procedure as guidelines.**
3. **Click on OK when you are finished editing parameters.**

DLSw Protocol Prioritization Parameter Descriptions

Use the following descriptions as guidelines when you configure parameters on the Global DLSw PP Parameters/Defaults window.

Parameter: **Protocol Priority (PP)**

Default: Disabled

Options: Enabled | Disabled

Function: Toggles protocol prioritization for configured DLSw peers on and off. If you set this parameter to Disabled, all default priority queues will be disabled. Setting this parameter to Disable is useful if you want to temporarily disable protocol prioritization for configured peers.

Instructions: Set to Disable if you want to temporarily disable all protocol prioritization activity. Set to Enable if you previously disabled protocol prioritization and now want to re-enable it.

Note: *Once you enable a peer-specific priority queue using the Peer Queues window, you must use that window to disable that peer's queues. You cannot disable queues that are already active from the Global DLSw PP Parameters/ Defaults window.*

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.17

Parameter: **PP for Unconfigured Peers**

Default: Disabled

Options: Enabled | Disabled

Function: Toggles protocol prioritization for unconfigured DLSw peers on and off. If you set this parameter to Disable, all unconfigured priority queues will be disabled. Setting this parameter to Disable is useful if you want to temporarily disable protocol prioritization for unconfigured peers.

Instructions: Set to Disable if you want to temporarily disable all protocol prioritization activity. Set to Enable if you previously disabled protocol prioritization and now want to re-enable it.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.20

Parameter:	**Max Queue Buffers for Unconfig Peers**
Default:	50
Range:	10 to 2147483647 packets
Function:	Specifies the maximum number of packets in each default queue.
Instructions:	Enter a number of packets to increase or decrease the default buffer size of 50 packets.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.21

Parameter:	**Max Queue Size for Unconfig Peers**
Default:	16000
Range:	5000 to 2147483647 bytes
Function:	Specifies the maximum size of each default queue.
Instructions:	Enter a number of bytes to increase or decrease the default queue size of 16000 bytes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.22

Parameter:	**Default Bandwidths**
Default:	60, 40, 0, 0, 0, 0, 0, 0, 0, 0
Range:	Ten entries (one per queue) of a percentage between 0 and 100.
Function:	Determines the number of default queues and allocates the bandwidth for each.
Instructions:	Either accept the default of 60 percent in Queue Number zero (Q0) and 40 percent in queue number one (Q1), or enter up to 10 values (one for each queue). Separate each bandwidth percent with a comma. The bandwidth percentages must total 100%. On low speed lines running NetBIOS, you should allocate 20% of the total bandwidth due to endstation timing. For example, the following specifies 10% of bandwidth allotted to each of 10 queues: **10, 10, 10, 10, 10, 10, 10, 10, 10, 10**
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.1.19

Configuring Peer-Specific Priority Queues

You create the priority queue configuration for all configured and unconfigured DLSw peers using the Global DLSw PP Parameters/Default window (refer to Figure 6-7).

You customize priority queues for particular configured DLSw peers using the Peer Queue Configuration window.

Note: *Peer-specific queue configurations take precedence over the default DLSw priority queue configuration.*

Priority Queues for a Specific DLSw Peer

Begin by displaying the Peer Queue Configuration window.

1. **From the Configuration Manager window, select Protocols→DLSw→Prot Prioritization (Outbound)→Peer Queue Entries.**

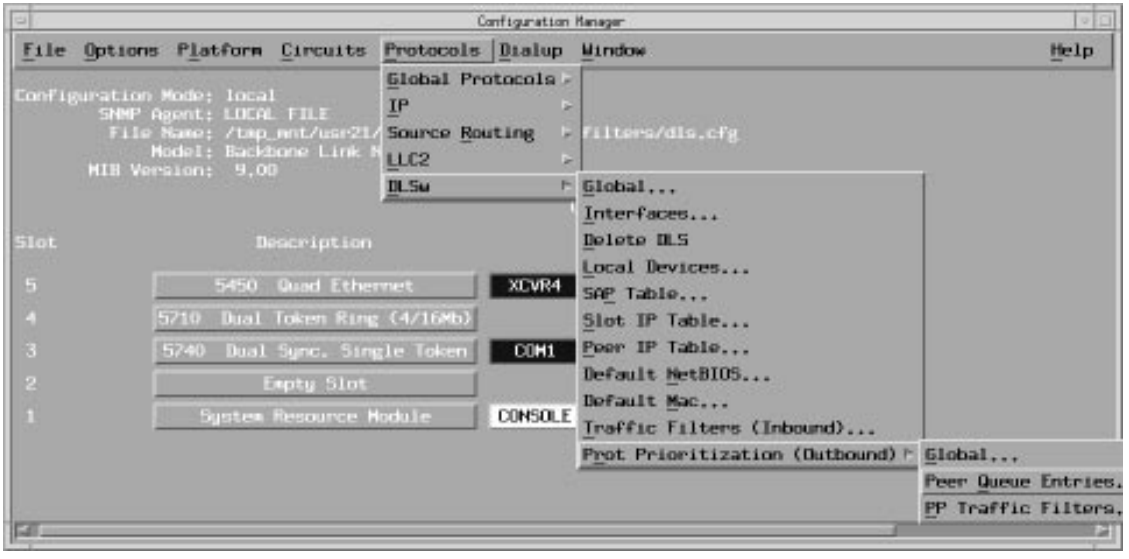


Figure 6-8. Selecting the Peer Queue Entries Window

The Peer Queue Configuration window appears (Figure 6-9).

Note: *See the later section* "Using the DLSw Peer Configuration Window" *for another way to access the Peer Queue Configuration window.*

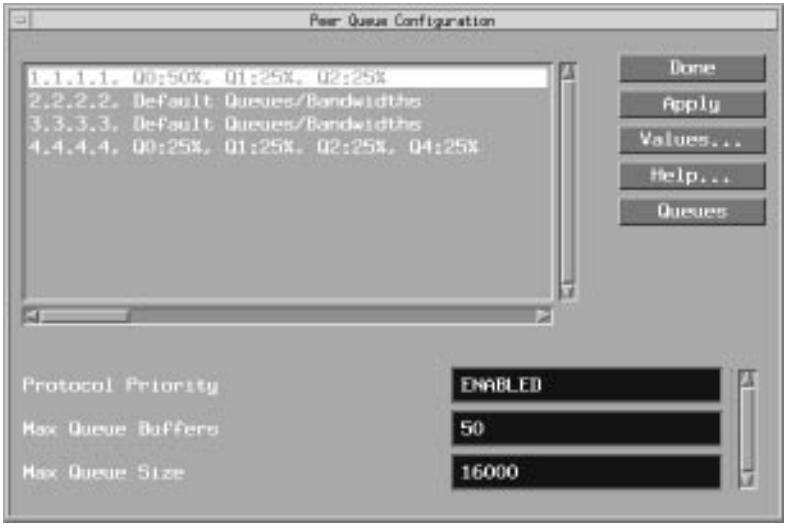


Figure 6-9. Peer Queue Configuration Window

The Peer Queue Configuration window summarizes the priority queue status for all DLSw peers. The scroll box lists each peer and indicates whether it uses the default or a specific queue configuration. (All of the DLSw peers in Figure 6-9 use the default queue configuration.)

The parameter boxes at the bottom of the screen show protocol prioritization as currently Disabled or Enabled for the selected peer, and list that peer's queue configuration information (queue buffers and size).

2. **Select the individual peer address on which to configure priority queues.**
3. **Click on Queues in the Peer Queue Configuration window.**

The Add/Edit/Delete Queues window appears (Figure 6-10).

Figure 6-10. Add/Edit/Delete Queues Window

4. Click on Add.

The Add Queue window appears (Figure 6-11).

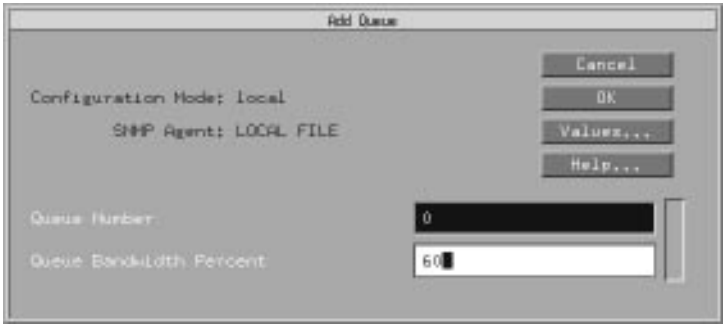


Figure 6-11. Add Queue Window

5. Enter a queue number.

The first queue must be queue number zero. You can number additional queues from 1 to 9. You do not need to number them in sequence, although doing so may help you keep track of the queues on a peer.

6. **Enter a bandwidth.**

   The bandwidth for queue number zero must be greater than 0. You can assign any percentage between 0 and 99 to subsequent queues, as long as the combined bandwidth for all queues totals 100 percent.

   On low speed lines running NetBIOS, you should allocate 20% of the total bandwidth due to endstation timing.

7. **Click on OK.**

   The Add/Edit/Delete Queues window reappears.

8. **Continue to add queues until the total bandwidth is 100 percent.**

   Repeat Steps 3 through 7 until the total bandwidth is 100 percent. Figure 6-12 shows a sample screen after adding queues.

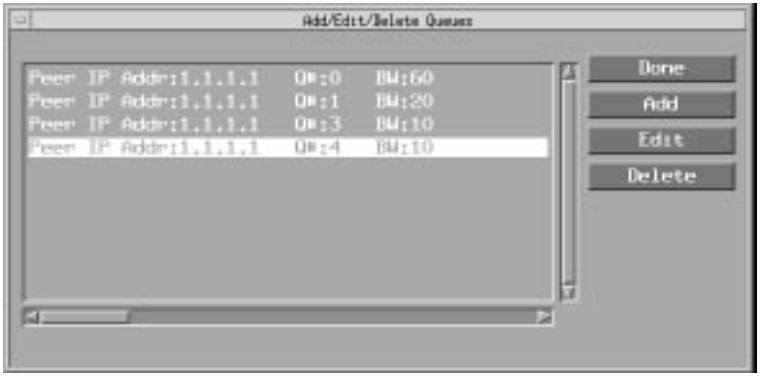


Figure 6-12. Configured Queues

9. **Click on Done.**

The Peer Queue Configuration window reappears (Figure 6-13). This time two of the DLSw peers use peer-specific queues and two use the default queue configuration.

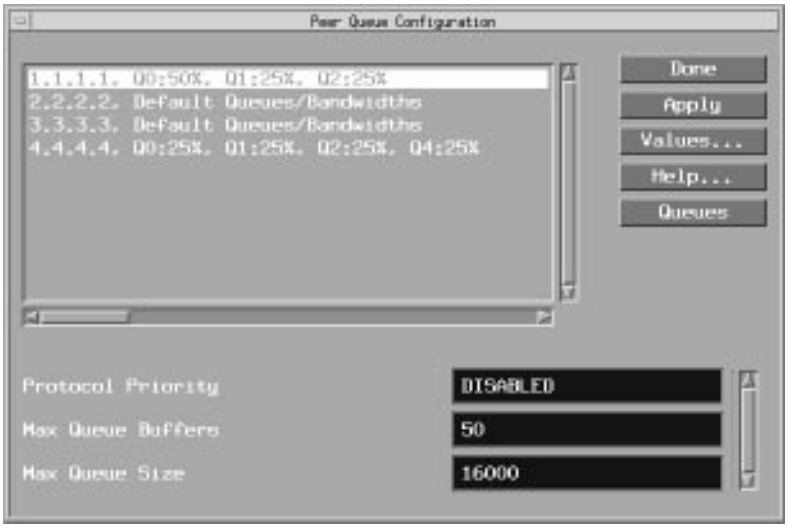


Figure 6-13. Peer Queue Configuration Window with Both Default and Peer-Specific Configurations

Enabling or Disabling a Single Peer's Priority Queues

You can enable or disable the queues you configured for an individual DLSw peer using the Peer Queue window.

Note: *Once you enable priority queues using the Peer Queue Configuration window, you must use that window to disable that peer's queues. You cannot disable queues that are already active from the Global DLSw PP Parameters/Default window.*

1. **From the Configuration Manager window, select Protocols→DLSw→Prot Prioritization (Outbound)→Peer Queue Entries (refer to Figure 6-8).**

   The Peer Queue Configuration window appears (see Figure 6-13).

2. **Select the peer from the scroll box.**

3. **Change the value of "Protocol Priority" to ENABLED or DISABLED.**
4. **Click on Apply.**
5. **Click on Done.**

Customizing Specific DLSw Peer Queues

Once you create and enable peer-specific queues, the DLSw peer in question uses default values that dictate how the priority queues work. You can change these values according to your network traffic needs.

1. **From the Configuration Manager window, select Protocols→DLSw→Prot Prioritization (Outbound)→Peer Queue Entries.**

   The Peer Queue Configuration window appears (Figure 6-14).

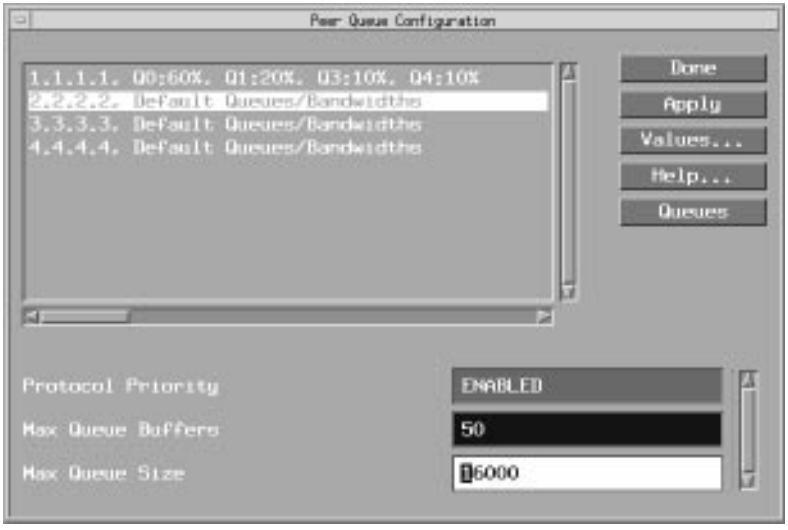


Figure 6-14. Peer Queue Configuration Window

2. **Edit the Peer Queue parameters you want to change, using the following descriptions as guidelines.**
3. **Click on Apply.**
4. **Click on Done.**

Peer Queue Configuration Parameter Descriptions

Use the following descriptions as guidelines when you configure parameters on the Peer Queue Configuration window.

Parameter:	**Protocol Priority**
Default:	Disabled
Options:	Enabled | Disabled
Function:	Toggles protocol prioritization on and off for this peer. If you set this parameter to Disable, priority filters will be disabled on this peer. Setting this parameter to Disable is useful if you want to temporarily disable protocol priority but leave the outbound filters in place.
Instructions:	Set to Disable if you want to temporarily disable all protocol prioritization activity on this peer. Set to Enable if you previously disabled protocol prioritization on this peer and now want to re-enable it.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.5.1.5

Parameter:	**Max Queue Buffers**
Default:	50
Range:	10 to 2147483647 packets
Function:	Specifies the maximum number of packets in each of this peer's queues.
Instructions:	Enter a number of packets to increase or decrease the default buffer size of 50 packets.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.5.1.6

Parameter:	**Max Queue Size**
Default:	16000
Range:	5000 to 2147483647 bytes
Function:	Specifies the maximum size of each of this peer's queues.
Instructions:	Enter a number of bytes to increase or decrease the default queue size of 16000 bytes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.5.5.1.7

Creating DLSw Priority Filters

Outbound traffic filters configured with the "queue" action (*priority filters*) determine which DLSw traffic is processed into priority queues.

To configure the DLSw priority filters, begin by displaying the DLS Priority/ Outbound Filters window.

1. **From the Configuration Manager window, select Protocols→DLSw→Prot Prioritization (Outbound)→PP Traffic Filters (Figure 6-15).**

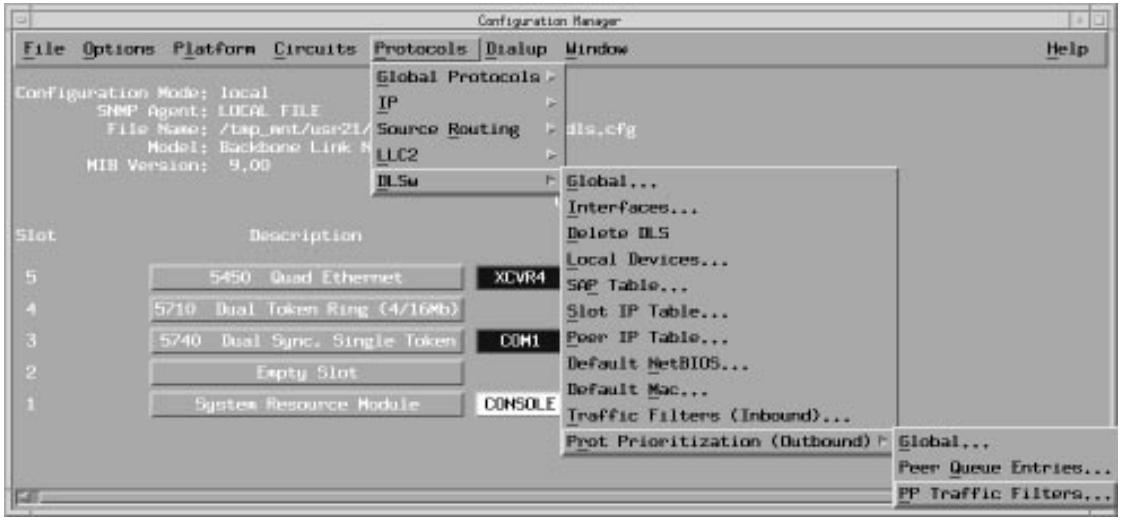


Figure 6-15. Selecting the DLS Priority/Outbound Filters Window

The DLS Priority/Outbound Filters window appears (Figure 6-16).

Note: *See the later section* "Using the DLSw Peer Configuration Window" *for another way to access the DLS Priority/Outbound Filters window.*

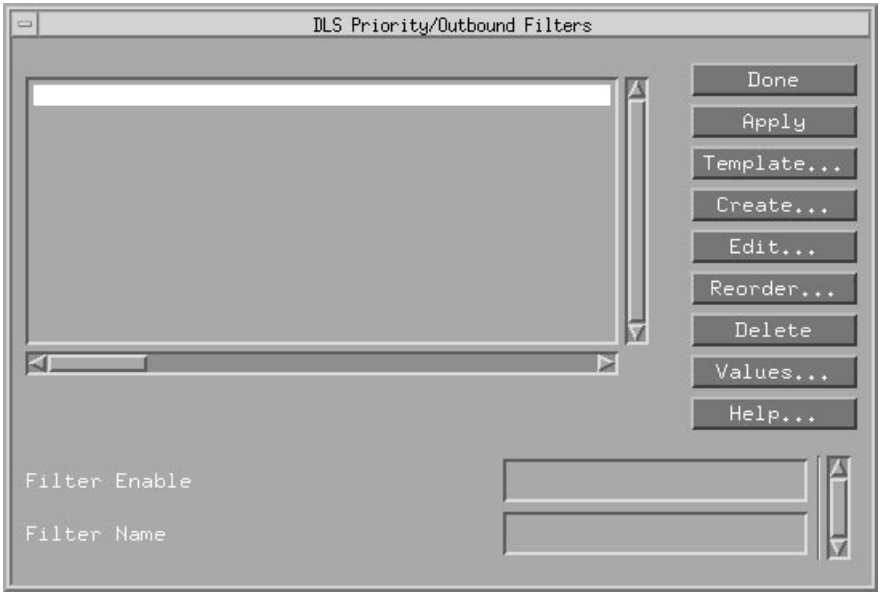


Figure 6-16. DLS Priority/Outbound Filters Window

This window shows any existing outbound traffic filters for DLSw peers, regardless of whether or not the filters are currently active on the peers.

2. **Click on Template.**

The Filter Template Management window appears (Figure 6-17).

If you are familiar with the Template Management window for WAN protocols, you create the templates for the DLSw priority filters window in the same way. See *Configuring Traffic Filters and Protocol Prioritization* for details about using the Priority/Outbound Filters window for WAN protocols.

Figure 6-17. Filter Template Management Window

The software includes sample templates for filtering NetBIOS and SNA traffic (*NetBIOS_Queue1* and *SNA_Queue0*, shown in Figure 6-17).

The sample templates place SNA traffic in Q0 and NetBIOS traffic in Q1. Unless you have customized the default queue configuration, Q0 (SNA) receives 60 percent of bandwidth and Q1 (NetBIOS) receives 40 percent of bandwidth. Using the remaining steps in this section, you can create filters from these, or similar, templates.

To use the sample templates, copy the file */usr/wf/template/template.flt* to the directory from which you start Site Manager (your Site Manager working directory). If that directory already contains a *template.flt* file, rename the existing file or copy the contents of the *template.flt* file into your *template.flt* existing file.

3. **Decide whether to create a new template or use an existing template.**

   More often than not you can use an existing filter template to build a new one.

   — If no existing template matches your needs, create a new filter template.

   — To create a template similar to an existing one, copy the existing template (to preserve the original template) to a new template with the same criteria and actions. Then, edit the new template.

— To modify an existing template without preserving the original template, edit the existing template. Note that changing a template does not affect interfaces to which the template has already been applied.

4. **Click on Create to make a new template, or select an existing template and click on Edit.**

   The Create DLS Template window or the Edit DLS Template window appears. Creating and editing templates involve the same steps; you use both windows in exactly the same way.

5. **Name the template.**

6. **Select a DLSw criterion (Figure 6-18).**

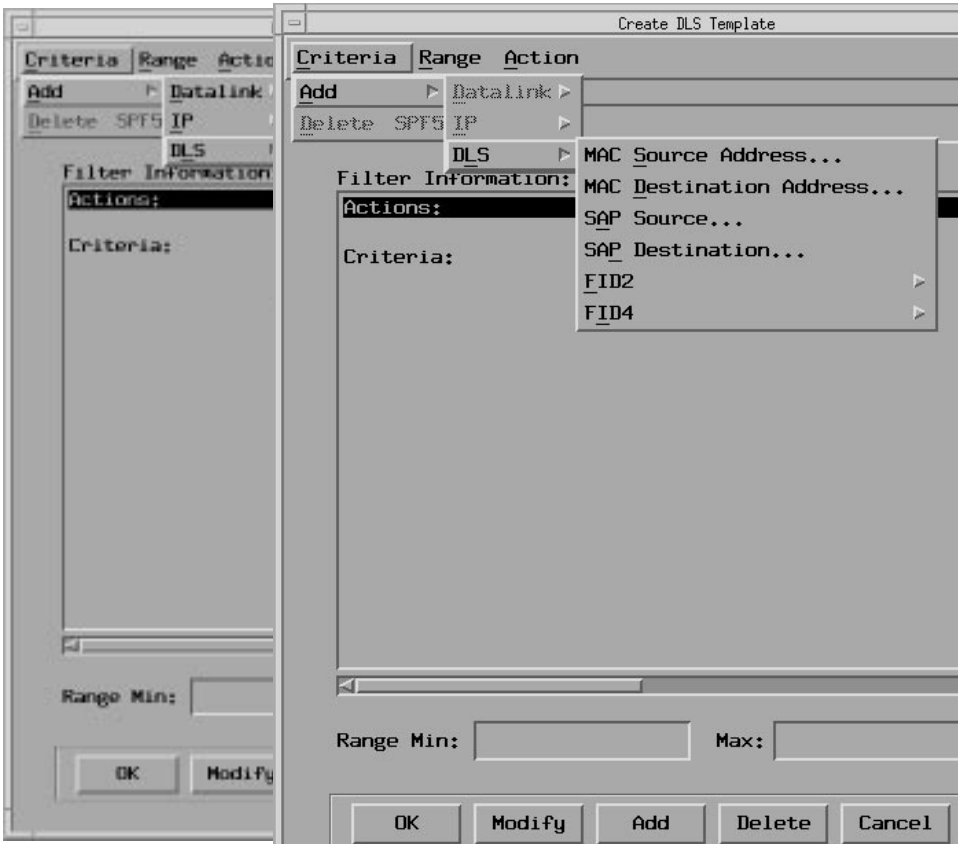


Figure 6-18. Selecting a Predefined DLSw Outbound Filter Criterion

Refer to Appendix B for information about the DLSw outbound traffic filter criteria.

7. **Select Action→Add→Queue (Figure 6-19).**

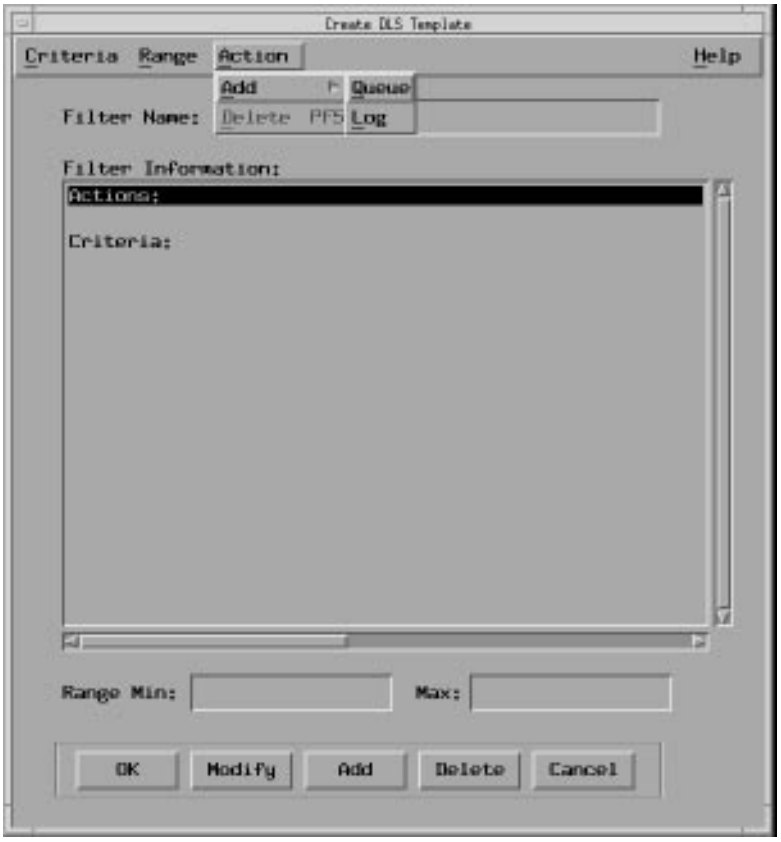


Figure 6-19. Selecting the DLSw Queue Action

The Queue Number window appears (Figure 6-20).

Figure 6-20. Queue Number Window

8. **Enter the queue number.**

   DLSw will send traffic that meets this filter's criteria and ranges to the queue number you specify here.

9. **Click on OK.**

   The Filter Template Management window reappears (refer to Figure 6-17).

10. **Click on Done to return to the DLS Priority/Outbound Filters window (refer to Figure 6-16).**

11. **To apply the template, click on Create.**

The Create Filter window appears (Figure 6-21).

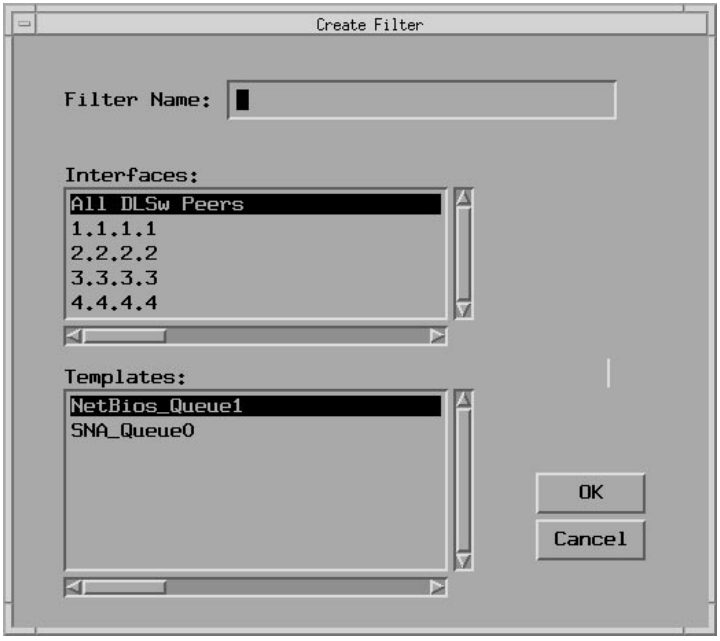


Figure 6-21. Create Filter Window

12. **Type a name for the filter in the Filter Name box.**
13. **Highlight All DLSw Peers to apply this template to all configured peers, or select an individual peer from the Interfaces scroll box.**
14. **Select the template you want to apply from the Templates scroll box.**
15. **Click on OK.**

    The DLS Priority/Outbound Filters window reappears, with the new filter displayed in the scroll box (Figure 6-22).
16. **Repeat Steps 11 through 15 to apply other templates.**

Each entry in the filter scroll box lists the filter number, filter name, and IP address of the affected DLSw peer. Filters that apply to all DLSw peers appear with IP address 0.0.0.0. Site Manager numbers the filters for each peer interface chronologically.

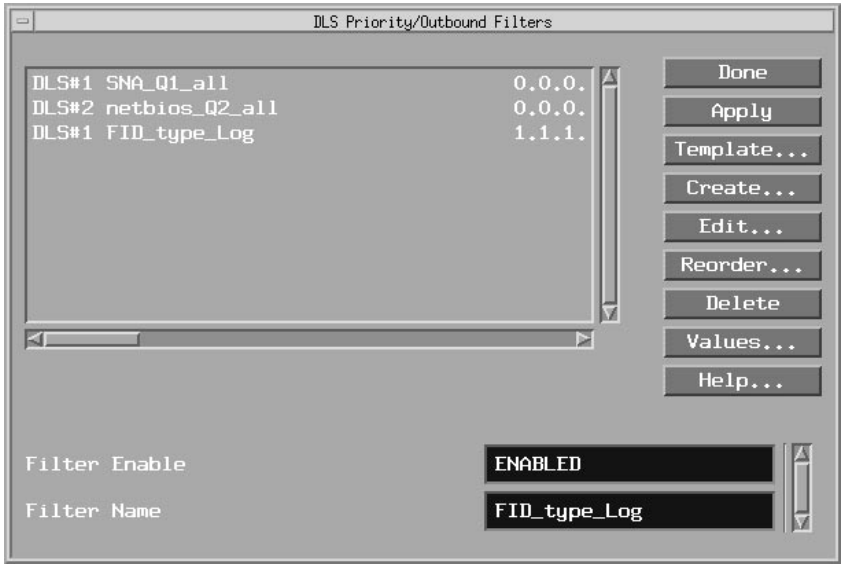


Figure 6-22. DLS Priority/Outbound Filters Window with Configured FIlters

Using the DLSw Peer Configuration Window

In addition to using the menu selections shown in this section, you can access the DLSw Protocol Prioritization windows directly from the DLSw Peer Configuration window (Figure 6-23).

To Access This Window	Click on This Button in the DLSw Peer Configuration Window
Global DLSw PP Parameters/Defaults	PP Global
Peer Queue Configuration	PP Queues
DLS Priority/Outbound Filters	PP Filters

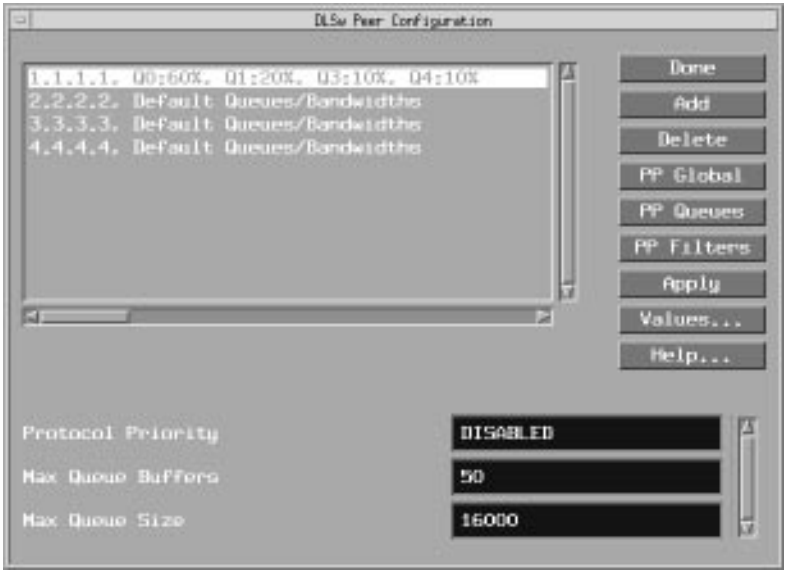


Figure 6-23. DLSw Peer Configuration Window

Sample Templates for DLSw Protocol Prioritization

In addition to using the Configuration Manager screens described in this guide to configure traffic filter templates, you can also edit or copy a traffic filter template using a text editor. The Configuration Manager stores all templates for all protocols in the file */usr/wf/template/template.flt*.

Included with the software is a *template.flt* file that contains two sample DLSw protocol prioritization templates you can use for differentiating SNA and NetBIOS traffic. To use the sample templates, copy */usr/wf/template/template.flt* to the directory from which you start Site Manager (your Site Manager working directory). If that directory already contains a *template.flt* file, copy the contents of the latest file into your existing file.

The sample templates place SNA traffic in the default queue (Q0) and NetBIOS traffic in Q1. Using the default queue configuration, Q0 receives 60 percent of bandwidth and NetBIOS receives 40 percent of bandwidth. The section “Creating DLSw Priority Filters” in this chapter lists the steps for creating filters from these, or similar, templates.

Appendix A
DLSw Default Settings

Tables A-1 through A-8 list the default settings for DLSw parameters. Use the Configuration Manager to edit the default settings.

Table A-1. DLSw Global Parameters

Parameter	Default
Enable	Enable
TCP Window Size	8000 (octets)
IP Virtual Ring	None
Max Slot Sessions	200 sessions per slot
Virtual Ring MTU	1500
MAC Cache Age	300 s
NetBIOS Cache Age	300 s
Reject Unconfigured Peers	Accept
Keepalive Time (sec)	60
Maximum Package Size	1532 bytes
Packaging Timeout	10 ms
Packaging Threshold	20 percent of TCP window size

Table A-2. DLSw Interface Parameters

Parameter	Default
Enable	Enable
Mode	Primary

Table A-3. DLSw Peer IP Table Parameters

Parameter	Default
Peer IP Address	None

Table A-4. DLSw Protocol Prioritization Parameters

Parameter	Default
Protocol Priority	Disabled
PP for Unconfigured Peers	Disabled
Max Queue Buffers for Unconfig Peers	50
Max Queue Size for Unconfig Peers	16000
Default Bandwidths	60,40, 0,0,0,0,0,0,0,0
Max Queue Buffers	50
Max Queue Size	16000
Queue Number	None
Queue Bandwidth Percent	0

Table A-5. DLSw Slot IP Table Parameters

Parameter	Default
IP Address for TCP Connection	None
Slot	None
IP Address	None

Table A-6. DLSw SAP Parameters

Parameter	Default
SAP Window	10 frames
SAP	None

Table A-7. DLSw Default NetBIOS Peer IP Table Parameters

Parameter	Default
Default NetBIOS Peer IP Address	None
NetBIOS Name	None
NetBIOS Peer IP Address	None

Table A-8. DLSw Default MAC Peer IP Table Parameters

Parameter	Default
Default MAC Peer IP Address	None
MAC Address	None
MAC Peer IP Address	None

Table A-9. DLSw Local Devices Parameters

Parameter	Default
Disable	Enable
PU Name	None
PU Type	None
IDBLOCK	None
IDNUM	None
XID Format	None
Source (Virtual) MAC (hex)	None
Source (Virtual) SAP (hex)	None
Destination (Host) MAC (hex)	None
Destination (Host) SAP (hex)	0x4
MAXOUT	7
MAXDATA	2057
Canureach Timer	30 s
Canureach Retries	4294967295
Link Station Timer	30 s
Link Station Retries	4294967295
SDLC Receive Credit	10
SDLC Transmit Credit	10

Appendix B
Criteria for DLSw Prioritization

This appendix includes both the DLSw *predefined* criteria that the Configuration Manager provides and the supported DLSw reference points for *user-defined* criteria for DLSw prioritization, described in Chapter 6.

Predefined DLSw Criteria

You configure outbound filters for DLSw traffic based on the predefined criteria listed in Table B-1.

Table B-1. Predefined Outbound Filter Criteria Based on DLSw Header

Packet Type or Component	Predefined Criteria
Any	MAC Source Address[1] MAC Destination Address[1] DSAP[2] SSAP[2]
FID4	FID Type Network Priority Trans Priority Dest Subarea Address Origin Subarea Address Expedited Flow Indicator Destination Element Origin Element User-Defined
FID2	FID Type EFI (Expedited Flow Indicator) Destination Element DAF (Destination Address Field) OAF (Origin Address Field) User-Defined

[1] See the “Specifying MAC Address Ranges” section later in this appendix.
[2] See the “Specifying Source and Destination SAP Code Ranges” section.

DLSw Reference Points

Tables B-2 and B-3 list the predefined DLSw reference points for outbound traffic filters based on the SNA Transmission Header.

Table B-2. DLSw Reference Points for FID2 Frames

Criteria (FID2)	Reference Point	Offset (bits)	Length (bits)
Format Identifier (FID)	SNA_START	0	4
Expedited Flow Indicator (EFI)	SNA_START	7	1
Destination Address Field (DAF)	SNA_START	16	8
Origin Address Field (OAF)	SNA_START	24	8

Table B-3. DLSw Reference Points for FID4 Frames

Criteria (FID4)	Reference Point	Offset (bits)	Length (bits)
Format Identifier (FID)	SNA_START	0	4
Network Priority	SNA_START	7	1
Transmission Priority Field (TPF)	SNA_START	30	2
Destination Subarea Address Field (DSAF)	SNA_START	64	32
Origin Subarea Address Field (OSAF)	SNA_START	96	32
Expedited Flow Indicator (EFI)	SNA_START	135	1
Destination Element Field (DEF)	SNA_START	144	16
Origin Element Field (OEF)	SNA_START	160	16

Specifying MAC Address Ranges

When you create a filter that includes a Source or Destination MAC Address criterion, you specify the MAC Address range in either most significant bit (MSB) or canonical format. Table B-4 lists the address formats to use.

Table B-4. Format for Specifying Source-Routing MAC Addresses

Address Type	Address Format
PPP	MSB
PPP	MSB
Bay Networks Standard Frame Relay	Canonical
Bay Networks Proprietary PPP	Canonical
Token Ring	MSB
Ethernet	Canonical

When defining outbound traffic filters you can specify a MAC address in either MSB or canonical format, but the default is canonical.

Source Routing Bridge Source MAC Addresses

When specifying Source MAC Source Routing addresses, set the most significant bit (MSB) to one.

For example (Token Ring packets):

1. The Source MAC address to be filtered is 0x40000037450440.
2. Add the First Bit Set MAC Address 0x800000000000.
3. Enter the filter criteria range as 0xC00037450440.

Bit 0 (the 0x80 bit) of Byte 0 (the leftmost byte) indicates the presence of the Routing Information Field (RIF). This bit is set to 1 if the RIF field is present and 0 if there is no RIF field. Keep this in mind if you use a sniffer to analyze packets for their Source MAC address. For example, a sniffer would decode LAA with the first byte of 40 as 0x400031740001. If the RIF bit is set, the hexadecimal value of the packet is 0xC00031740001.

Source Routing Bridge Functional MAC Addresses

Functional MAC addresses are Destination MAC addresses that always conform to the following rules:

- Byte 0 = 0xC0
- Byte 1 = 0x00
- The first half of byte 2 = 0x0 - 0x7

Table B-5 lists some common functional MAC addresses.

Table B-5. Functional MAC Addresses

Function Name	MAC Address (MSB)	Identifying Bit	Ethernet Address
Active Monitor	0xC000 0000 0001	Byte 5, bit 7	0x030000000080
Ring Parameter Server	0xC000 0000 0002	Byte 5, bit 6	0x030000000040
Ring Error Monitor	0xC000 0000 0008	Byte 5, bit 4	0x030000000010
Configuration Report Server	0xC000 0000 0010	Byte 5, bit 3	0x030000000008
NetBIOS	0xC000 0000 0080	Byte 5, bit 0	0x030000000001
Bridge	0xC000 0000 0100	Byte 4, bit 7	0x030000008000
LAN Manager	0xC000 0000 2000	Byte 4, bit 2	0x030000000400
User-defined	0xC000 0008 0000 to 0xC000 4000 0000	Byte 3, bits 0-4; Byte 2, bits 1-7	0x030000100000 to 0x030002000000

Specifying Source and Destination SAP Code Ranges

Table B-6 lists several SAP codes to use when specifying a range for Source or Destination SAP traffic filter criteria.

Table B-6. SAP Codes

Description	SAP Code
XID or TEST	00
Individual Sublayer Mgmt	02
Group Sublayer Mgmt	03
SNA	04, 08, 0C
IP	06
Proway Network Mgmt	0E
Novell and SDLC Link Servers	10
CLNP ISO OSI	20, 34
BPDU	42
X.25 over 802.2 LLC2	7E
XNS	80
Nestar	86
Active station list	8E
ARP	98
SNAP Subnet Access Protocol	AA
Banyan VIP	BC
Novell IPX	E0
CLNP ISO OSI	EC
IBM NetBIOS	F0
LAN Manager	F4, F5
Remote Program load	F8
UB	FA
IBM RPL	FC
ISO Network Layer	FE
LLC broadcast	FF

Index

A

actions, traffic filter
  DLSw protocol prioritization, 6-27
adding
  DLSw default MAC peer IP entries, 5-39
  DLSw default NetBIOS peer IP entries, 5-33
  DLSw local devices, 3-14
  DLSw peer IP entries, 5-18
  DLSw SAP entries, 5-27
  DLSw slot entries, 5-22
address
  learning capabilities, 3-15, 3-16
  MAC, 3-15
  peer IP, 3-10, 3-16, 3-17, 5-20, 5-23

B

Bay Networks
  CompuServe forum, xviii
  customer support, xviii
  Home Page on World Wide Web, xix
  InfoFACTS service, xix
  publications, ordering, xxi
  Technical Response Center, xx
bridging services
  translation bridge, 2-13
  translation bridge on an SRB circuit, 2-11
  transparent bridge, 2-12 to 2-13
broadcast peers, 3-10

C

Cable Type parameter, 4-16
Canureach Retries parameter, 4-24, 5-52
Canureach Timer parameter, 4-23, 5-52
Circuit Definition window, 5-16
Circuit List window, 5-15
circuitless IP, used as a DLSw peer IP address, 5-21
Clock Source parameter, 4-14
CompuServe, Bay Networks forum on, xviii
Configuration Manager window, 5-3
configuration overview, 3-1
configuration roadmaps, 3-2 to 3-4
configured peers, 5-1
congestion control, DLSw protocol prioritization, 6-7
criteria
  DLSw protocol prioritization, 6-26
customer support. *See* getting help

D

Data Link Switching (DLSw).
  See DLSw
Default MAC Peer IP Address parameter, 5-43
Default NetBIOS Peer IP Address parameter, 5-37
Default Queue Bandwidths parameter, 6-14
defaults, DLSw parameters, A-1
deleting
  DLSw default MAC peer IP entries, 5-43
  DLSw default NetBIOS peer IP entries, 5-37
  DLSW from a node, 5-54
  DLSw local device entries, 5-54

DLSw peer IP entries, 5-20
DLSw SAP entries, 5-31
DLSw slot entries, 5-25
dequeuing
algorithms, weighted dequeuing, 6-5
DLSw protocol prioritization, 6-4
Destination (Host) MAC (hex) parameter, 4-22, 5-50
Destination (Host) SAP (hex) parameter, 4-22, 5-51
Disable parameter, 4-19, 5-47
DLCI parameter, 4-6
DLS Local Device Configuration window, 5-45
DLSw
accessing parameters, 5-2
and other protocols, 1-14
bridging services
source routing, 2-11
translation bridge, 2-13
translation bridge on an SRB circuit, 2-11
transparent bridge, 2-12 to 2-13
communication over TCP/IP, 1-6 to 1-7
configuration objects
for dual switch operation, 3-8 to 3-12
for SDLC operation, 3-12 to 3-15
for single switch operation, 3-5 to 3-8
optional, 3-15 to 3-17
configuration overview, 3-1 to 3-15
Default NetBIOS Peer IP Table parameters, 5-32 to 5-38
defaults, A-1 to A-4
enabling DLSw, 4-1
inbound traffic filters, 1-13
interface parameters, 5-13 to 5-17
LLC2 media support, 1-3
Local Devices parameters, 4-18 to 4-25, 5-44 to 5-53
media support for, 1-3
networking overview, 1-2 to 1-3
Peer IP Table parameters, 5-17 to 5-21
peers
defined, 3-9
defining in a TCP/IP network, 3-9 to 3-11
multiple, 2-11
unconfigured, 3-11
performance considerations, 2-18
priority queues, 6-3
protocol prioritization, 1-13
related publications, 1-15
remote NetBIOS/SNA systems, 3-15 to 3-17
SAP table parameters, 5-26 to 5-32
SAPs, defined, 3-5
SDLC media support, 1-3
single and dual switch services, 1-3 to 1-4
Slot IP Table parameters, 5-21 to 5-26
DLSw Default MAC Peer IP Table Parameters
MAC Peer IP Address, 5-41
DLSw Default MAC Peer IP Table parameters
Default MAC Peer IP Address, 5-43
MAC Address, 5-41
DLSw default NetBIOS peer IP parameters
NetBIOS Name, 5-35
NetBIOS Peer IP Address, 5-35
DLSw Default NetBIOS Peer IP Table parameters
Default NetBIOS Peer IP Address, 5-37
DLSw default settings, A-1
DLSw global parameters
Enable, 5-5
IP Virtual Ring, 5-7
Keepalive Timer, 5-11
Max Cache Age, 5-9
Max Slot Sessions, 5-8
Maximum Package Size, 5-12
NetBIOS Cache Age, 5-9
Packaging Threshold, 5-12
Packaging Timeout, 5-12
Reject Unconfigured Peers, 5-10
TCP Window Size, 5-6
Virtual Ring MTU, 5-8
DLSw Interface Configuration window, 5-13
DLSw interface parameters
Enable, 5-14

DLSw local devices parameters
Canureach Retries, 4-24, 5-52
Canureach Timer, 4-23, 5-52
Destination (Host) MAC (hex), 4-22, 5-50
Destination (Host) SAP (hex), 4-22, 5-51
Disable, 4-19, 5-47
Link Address (hex), 4-18, 5-47
Link Station Retries, 4-24, 5-53
Link Station Timer, 4-24, 5-52
MAXDATA, 4-23, 5-51
MAXOUT, 4-23, 5-51
PU IDBLOCK, 4-20, 5-48
PU IDNUM, 4-20, 5-49
PU Name parameter, 4-19, 5-47
PU Type, 4-19, 5-48
SDLC Receive Credit, 4-25, 5-53
SDLC Transmit Credit, 4-25, 5-53
Source (Virtual) MAC (hex), 4-21, 5-50
Source (Virtual) SAP (hex), 4-22, 5-50
XID Format, 4-21, 5-49
DLSw MAC Peer Configuration window, 5-39, 5-42, 5-43
DLSw NetBIOS Configuration window, 5-34
DLSw NetBIOS Peer Configuration window, 5-33, 5-36, 5-38
DLSw packaging, 2-18
configuring, 5-12
DLSw parameters, using descriptions for, 5-1
DLSw Peer Configuration window, 4-10, 5-18, 5-19, 5-20
DLSw Peer IP Table parameters
Peer IP Address, 5-19
DLSw Protocol Prioritization
Default Queue Bandwidths parameter, 6-14
Max Queue Buffers for Unconfig Peers parameter, 6-14
Max Queue Buffers parameter, 6-21
Max Queue Size for Unconfig Peers parameter, 6-14
Max Queue Size parameter, 6-22
PP for Unconfigured Peers parameter, 6-13
Protocol Priority parameter, 6-13, 6-21
DLSw SAP Configuration window, 4-12, 5-27, 5-30, 5-32
DLSw SAP Table parameters
SAP, 5-28
SAP Window, 5-31
DLSw Slot Configuration window, 4-8, 5-22, 5-24, 5-25
DLSw Slot IP Table parameters
IP Address, 5-23
IP Address for TCP Connection, 5-25
DLSw slot IP table parameters
Slot, 5-23
dual switch SDLC conversion, 1-10
dual switch services, 1-3 to 1-4

E

Edit Circuits function, editing DLSw interface parameters with, 5-14 to 5-17
Edit Connector window, 5-15
Edit DLSw Global Parameters window, 5-4
Edit DLSw Interface window, 5-16
editing
DLSw Default MAC Peer IP Table parameters, 5-38 to 5-44
DLSw Default NetBIOS Peer IP Table parameters, 5-32 to 5-38
DLSw global parameters, 5-3 to 5-12
DLSw interface parameters, 5-13 to 5-17
DLSw local devices parameters, 5-44 to 5-53
DLSw Peer IP Table parameters, 5-17 to 5-21
DLSw SAP Table parameters, 5-26 to 5-32
DLSw Slot IP Table parameters, 5-21 to 5-26
template.flt file, 6-31
Enable
global parameter, 5-5
interface parameter, 5-14
enabling DLSw services, 4-1 to 4-26

Ethernet/802.3, multiple DLSw peers serving a LAN, 2-11
explorer frames, 2-11

F

filters, DLSw inbound and outbound, 1-13
flow control, 2-17
  configuration parameters for, 4-25, 5-29, 5-53
  LLC, 2-17
  TCP, 2-17
Frame Relay Mapping Add window, 4-6
Frame Relay Mappings window, 4-5
Frame Relay support, 1-11 to 1-12

G

getting help
  from a Bay Networks Technical Response Center, xx
  through CompuServe, xviii
  through InfoFACTS service, xix
  through World Wide Web, xix

I

IBM 6611 Network Processor, 1-2
IDBLOCK parameter, 4-20, 5-48
IDNUM parameter, 4-20, 5-49
inbound traffic filters, 1-13
InfoFACTS service, xix
Internal Clock Speed parameter, 4-15
IP Address for TCP Connection parameter, 5-25
IP Address parameter, 4-9, 5-23
IP virtual ring, 2-3 to 2-6
IP Virtual Ring parameter, 4-3, 4-4, 5-7, 5-9
IP, using the circuitless IP address, 5-21

K

Keepalive Timer parameter, 5-11

L

learning capabilities, 3-15
Link Address (hex) parameter, 4-18, 5-47
Link Station Retries parameter, 4-24, 5-53
Link Station Timer parameter, 4-24, 5-52
link stations
  roles, 1-8
LLC
  flow control, 2-17
LLC2 Frame Relay Mapping Add window, 4-6
LLC2 Frame Relay Mappings window, 4-5
LLC2 media support, 1-3
LLC2 over Frame Relay, 1-11 to 1-12
local devices
  adding, 3-14, 4-17
  editing parameters for, 5-44
Local MAC parameter, 4-7

M

MAC Address parameter, 5-41
MAC Cache Age parameter, 5-9
MAC Peer IP Address parameter, 5-41
Max Queue Buffers for Unconfig Peers parameter, 6-14
Max Queue Buffers parameter, 6-21
Max Queue Size for Unconfig Peers parameter, 6-14
Max Queue Size parameter, 6-22
Max Slot Sessions parameter, 2-14, 5-8
MAXDATA parameter, 4-23, 5-51
Maximum Package Size parameter, 5-12
MAXOUT parameter, 4-23, 5-51

memory requirements, 2-14
multiple DLSw peers, 2-11

N

negotiable link stations, 1-8
NetBIOS
  sample template, 6-31
NetBIOS Cache Age parameter, 5-9
NetBIOS Name parameter, 5-35
NetBIOS Peer IP Address parameter, 5-35
NetBIOS, sample template, 6-24

P

packaging, 2-18
  configuring, 5-12
Packaging Threshold parameter, 5-12
Packaging Timeout parameter, 5-12
parallel data paths
  avoiding, 2-9
  in SRB topology, 2-10
  in transparent bridge topology, 2-9
peer IP address, 3-9
Peer IP Address parameter, 4-11, 5-19
peer, DLSw
  configuring queues, 6-15
  defined, 3-9
  enabling protocol prioritization, 6-11
peers
  configured, 5-1
  defined, 3-9
  learning mechanism, 3-15
  multiple, 2-11
performance considerations, 2-18
  DLSw packaging, 2-18
PP for Unconfigured Peers parameter, 6-13
primary link stations, 1-8
priority queues. *See* queues, priority
protocol prioritization, 1-13, 5-54
  clipped packets, 6-7
  Default Queue Bandwidths parameter, 6-14
  defined, 6-1
  described, 6-1
  DLSw, 6-1 to 6-31
    accessing, 6-9, 6-30
    Add Queue window, 6-17
    Create Filter window, 6-28
    dequeuing, 6-4
    DLSw Priority/Outbound Filters window, 6-23
    Filter Template Management window, 6-24
    Global DLSw PP Parameters/Defaults Window, 6-10
    how it works, 6-3
    Peer Queue Configuration window, 6-16
    Queue Number window, 6-27
    selecting an action, 6-27
    selecting criteria, 6-26
  Max Queue Buffers for Unconfig Peers parameter, 6-14
  Max Queue Buffers parameter, 6-21
  Max Queue Size for Unconfig Peers parameter, 6-14
  Max Queue Size parameter, 6-22
  PP for Unconfigured Peers parameter, 6-13
  Protocol Priority parameter, 6-13, 6-21
  queue depth, 6-7
  tuning, 6-7
  usefulness of, 6-1
Protocol Priority parameter, 6-13, 6-21
PU Name parameter, 4-19, 5-47
PU Type parameter, 4-19, 5-48

Q

queue depth, DLSw protocol prioritization, 6-7
queues, priority
  about, 6-2
  DLSw, 6-3
    configuring, 6-22
    configuring default, 6-12

configuring peer-specific, 6-15
enabling and disabling, 6-19
DLSw enqueuing, 6-4

R

Reject Unconfigured Peers parameter, 5-10
Remote MAC parameter, 4-7
RFC 1490 Frame Relay standard, 1-11
RTS Enable parameter, 4-16

S

SAP address
in a TEST frame, 2-12
in an explorer frame, 2-11
SAP parameter, 4-13, 5-28
SAP Window parameter, 5-31
SAP window, purpose of, 2-17
SAPs, defined, 3-5
SDLC
enabling DLSw over, 4-13 to 4-16
supported interfaces, 1-8
topologies, 1-8
SDLC conversion, 1-8 to 1-11
SDLC Line Parameters window, 4-14
SDLC Receive Credit parameter, 4-25, 5-53
SDLC Transmit Credit parameter, 4-25, 5-53
secondary link stations, 1-8
Select Protocols window, 4-16
single-switch SDLC conversion, 1-9 to 1-11
single-switch services, 1-3 to 1-4
Slot parameter, 4-9, 5-23
SNA
sample template, 6-31
SNA, sample template, 6-24
Source (Virtual) MAC (hex) parameter, 4-21, 5-50
Source (Virtual) SAP (hex) parameter, 4-22, 5-50
Source Route Bridge
topology considerations, 2-1 to 2-9
computing DLSw connection path, 2-8 to 2-9
counting DLSw bridge, 2-7
counting internal LANS, 2-7
counting SRB LANs and bridges, 2-2 to 2-3
internal LANS, 2-6 to 2-7
IP virtual rings, 2-3 to 2-6
Sync Line Coding parameter, 4-15
Synchronous parameters
Cable Type, 4-16
Clock Source, 4-14
Internal Clock Speed, 4-15
RTS Enable, 4-16
Sync Line Coding, 4-15

T

TCP Window Size parameter, 5-6
TCP/IP, DLSw communications over, 1-6 to 1-7
Technician Interface, 5-1
template.flt file
editing, 6-31
sample, 6-24, 6-31
templates
changing after applying to a filter, 6-25
sample, 6-24
TEST frames, 2-12
Token Ring-to-Ethernet topology considerations, 5-9
traffic filter criteria, B-1 to B-6
traffic filters, 5-54
DLSw and outbound, 1-13
outbound
Create Filter window, 6-28
creating DLSw templates, 6-24
DLSw interfaces, 6-22
DLSw Priority/Outbound Filters window, 6-23

Filter Template Management window, 6-24
media and protocols supported, 6-1
Queue Number window, 6-27
translation bridge support, 2-13
transparent bridge support, 2-12

U

unconfigured peers, 3-10

V

virtual ring, 2-3 to 2-6
Virtual Ring MTU parameter, 2-5, 4-4, 5-7, 5-8, 5-9

W

weighted dequeuing algorithm, 6-5
window size, SAP, 5-31
World Wide Web, Bay Networks Home Page on, xix

X

XID Format parameter, 4-21, 5-49